
GAZİ ÜNİVERSİTESİ
Gazi
1926

KAMU KURUMLARININ BİLGİ GÜVENLİĞİ POLİTİKALARININ KURUMSAL BİLGİ GÜVENLİĞİNİN SAĞLANMASI AÇISINDAN ETKİNLİĞİNİN ANALİZ EDİLMESİ

Samime MERAL

YÜKSEK LİSANS TEZİ
BİLGİ GÜVENLİĞİ MÜHENDİSLİĞİ ANA BİLİM DALI

GAZİ ÜNİVERSİTESİ
FEN BİLİMLERİ ENSTİTÜSÜ

HAZİRAN 2022

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.

İmza
Samime MERAL
09/06/2022

KAMU KURUMLARININ BİLGİ GÜVENLİĞİ POLİTİKALARININ KURUMSAL BİLGİ GÜVENLİĞİNİN SAĞLANMASI AÇISINDAN ETKİNLİĞİNİN ANALİZ EDİLMESİ

(Yüksek Lisans Tezi)

Samime MERAL

GAZİ ÜNİVERSİTESİ
FEN BİLİMLERİ ENSTİTÜSÜ

Haziran 2022

ÖZET

Bu çalışma ile kurumların bilgi güvenliğini sağlamaya yönelik yapmış olduğu çalışmaların ve bu doğrultuda hazırlamış oldukları bilgi güvenliği politikalarının kurumsal bilgi güvenliğinin sağlanması açısından mevcut durumunun tespit edilmesi amaçlanmıştır. Kurumların sahip olduğu verilerin kritiklik düzeyleri ve iş süreçlerinde bilgi sistemleri kullanılma yoğunluğu değişkenleri belirlenerek, bu değişkenlere göre kurumların sahip olduğu bilgi güvenliği politikalarının etkinliğinin istatistiksel açıdan anlamlı düzeyde bir farklılık gösterip göstermeyeceği konusu üzerine odaklanılmıştır. Kamu kurumlarının bilgi güvenliği politikalarının analiz edilmesi amacıyla kritiklik durumlarına göre örneklem yöntemiyle seçilen kamu kurumlarında bilgi teknolojileri/güvenliği alanında farklı branşlarda 121 çalışanın katılımıyla anket çalışması gerçekleştirilmiştir. Veri toplama aracı olarak araştırmacı tarafından 55 soruluk bir anket hazırlanmıştır. Hazırlanan anket üç bölümden oluşmaktadır. Anketin birinci bölümünde katılımcıların demografik bilgilerini anlamaya yönelik sorular, ikinci bölümünde katılımcıların görev aldığı kurumun kurumsal yapısını anlamaya yönelik sorular ve son bölümünde ise bilgi güvenliği politikalarının etkinliğini ölçmeye yönelik hazırlanan 48 sorudan oluşan 5'li likert tipi sorular yer almaktadır. Elde edilen veriler bilgisayar ortamında SPSS 28.0 istatistik paket programı aracılığıyla çözümlenerek karşılaştırmalar yapılmıştır. Geçerlik güvenirlik analizi sonucu Cronbach Alpha (α) güvenirlik katsayısı anketin tümü için ,96 olarak hesaplanmıştır. Verilere uygulanan Kolmogorov-Smirnov ve Shapiro-Wilk normallik testleri sonucunda p anlamlılık değeri 0,05 anlamlılık değerinin üzerinde olduğu için verilerin normal dağıldığı hipotezi kabul edilerek normal dağılan veriler için uygulanan parametrik testler tercih edilmiştir. Verilerin analizi için tanımlayıcı istatistiksel analizler ve üç ya da daha fazla grup karşılaştırması için tek yönlü varyans analizi tekniği kullanılmıştır. Araştırma sonucunda, anketteki tüm sorular değerlendirildiğinde kurumların bilgi güvenliği politikalarının %77,80 oranında etkin olduğu ve kurumların sahip olduğu verilerin kritiklik düzeyleri ve iş süreçlerinde bilgi sistemleri kullanılma yoğunluğuna göre kurumların bilgi güvenliği politikalarının etkinliği arasında istatistiksel açıdan anlamlı düzeyde farklılık olduğu görülmüştür. Ayrıca kurumların sahip olduğu verilerin kritiklik düzeyleri arttıkça bilgi güvenliği politikalarının etkinliğinin arttığı sonucuna varılmıştır.

Bilim Kodu	:	92403
Anahtar Kelimeler	:	Bilgi güvenliği, kurumsal bilgi güvenliği, bilgi güvenliği politikaları, bilgi güvenliği yönetim sistemi
Sayfa Adedi	:	89
Danışman	:	Prof. Dr. Halil İbrahim BÜLBÜL

ANALYSIS OF THE EFFICIENCY OF THE INFORMATION SECURITY POLICIES OF PUBLIC INSTITUTIONS IN TERMS OF ENSURING CORPORATE INFORMATION SECURITY

(M. Sc. Thesis)

Samime MERAL

GAZİ UNIVERSITY

GRADUATE SCHOOL OF NATURAL AND APPLIED SCIENCES

June 2022

ABSTRACT

With this study, it is aimed to determine the current situation of the studies carried out by the institutions to ensure information security and the information security policies they have prepared in this direction in terms of ensuring corporate information security. By determining the variables of the criticality level of the data owned by the institutions and the intensity of using information systems in business processes, it has been focused on whether the effectiveness of the information security policies of the institutions will show a statistically significant difference according to these variables. In order to analyze the information security policies of public institutions, a survey was conducted with the participation of 121 employees from different branches in the field of information technologies / security in public institutions selected by sampling method according to their criticality. A 55-question questionnaire was prepared by the researcher as a data collection tool. The prepared questionnaire consists of three parts. In the first part of the questionnaire, there are questions to understand the demographic information of the participants, in the second part there are questions to understand the institutional structure of the institution where the participants work, and in the last part, there are 5-point Likert type questions consisting of 48 questions prepared to measure the effectiveness of information security policies. The obtained data were analyzed using the SPSS 28.0 statistical package program in the computer environment and comparisons were made. As a result of the validity and reliability analysis, the Cronbach Alpha (α) reliability coefficient was calculated as .96 for the entire questionnaire. As a result of the Kolmogorov-Smirnov and Shapiro-Wilk normality tests applied to the data, since the p significance value was above the 0.05 significance value, the hypothesis that the data were normally distributed was accepted and parametric tests applied for the normally distributed data were preferred. Descriptive statistical analyzes were used for data analysis and one-way analysis of variance technique was used for comparison of three or more groups. As a result of the research, when all the questions in the questionnaire were evaluated, it was seen that the information security policies of the institutions were effective at the rate of 77.80% and there was a statistically significant difference between the effectiveness of the information security policies of the institutions according to the criticality levels of the data owned by the institutions and the intensity of the use of information systems in business processes. In addition, it has been concluded that the effectiveness of information security policies increases as the criticality levels of the data owned by the institutions increase.

Science Code	:	92403
Key Words	:	Information security, corporate information security, information security policies, information security management system
Page Number	:	89
Supervisor	:	Prof. Dr. Halil İbrahim BÜLBÜL

TEŞEKKÜR

Çalışmam boyunca yardım ve katkılarıyla beni yönlendiren ve desteğini esirgemeyen değerli hocam, tez danışmanım Sayın Prof. Dr. Halil İbrahim BÜLBÜL'e, Yüksek Lisans eğitimim süresince farklı bilgiler ve fikirler edindiğim Gazi Üniversitesi Fen Bilimleri Enstitüsü Bilgi Güvenliği Mühendisliği Ana Bilim Dalı çok değerli öğretim üyelerine ve aynı dönem eğitim gördüğüm bölüm arkadaşlarıma, çalışmama gönüllü olarak katılım sağlayan kamu çalışanlarına, hayatımın her evresinde yanımda olan ve beni her zaman destekleyen sevgili aileme ve sabırla, maddi manevi her türlü desteğiyle benim her zaman yanımda olan çok değerli eşim Erkan MERAL'e teşekkür ve şükranlarımı sunarım.

İÇİNDEKİLER

Sayfa

Sayfa

ÇİZELGELERİN LİSTESİ

Çizelge **Sayfa**

Çizelge **Sayfa**

SİMGELER VE KISALTMALAR

Bu çalışmada kullanılmış kısaltmalar, açıklamaları ile birlikte aşağıda sunulmuştur.

Kısaltmalar	Açıklamalar
BG	Bilgi Güvenliği
BGP	Bilgi Güvenliği Politikası
BGYR	Bilgi Güvenliği Yönetimi Rehberi
BGYS	Bilgi Güvenliği Yönetim Sistemi
BİLGEM	Bilişim ve Bilgi Güvenliği İleri Teknolojiler Araştırma Merkezi
BSI	İngiliz Standartlar Enstitüsü (British Standards Institute)
CB	Cumhurbaşkanlığı
CB DDO	Cumhurbaşkanlığı Dijital Dönüşüm Ofisi
KamuNet	Kamu Sanal Ağı
KAYSİS	Elektronik Kamu Bilgi Yönetim Sistemi
KPMG	Klynveld Peat Marwick Goerdeler
ISO	Uluslararası Standardizasyon Örgütü (International Organization for Standardization)
ISO 27001	ISO/IEC 27001 Bilgi Güvenliği Yönetim Sistemi Standardı
ISO 27002	ISO/IEC 27002 Bilgi Güvenliği Kontrolleri İçin Uygulama Prensipleri Standardı
REHBER	Bilgi ve İletişim Güvenliği Rehberi
SGE	Siber Güvenlik Enstitüsü
SOME	Siber Olaylara Müdahale Ekibi
TOBB	Türkiye Odalar ve Borsalar Birliği
TSE	Türk Standardları Enstitüsü
TÜBİTAK	Türkiye Bilimsel ve Teknolojik Araştırma Kurumu
T.C.	Türkiye Cumhuriyeti
UAB	Ulaştırma ve Altyapı Bakanlığı
UEKAE	Ulusal Elektronik ve Kriptoloji Araştırma Enstitüsü
UDHB	Ulaştırma, Denizcilik ve Haberleşme Bakanlığı

Kısaltmalar	Açıklamalar
UNESCAP	Birleşmiş Milletler Asya ve Pasifik İktisadi ve Sosyal Komisyonu (The United Nations Economic and Social Commission for Asia and the Pacific)
YTE	Yazılım Teknolojileri Araştırma Enstitüsü

1. GİRİŞ

Bilgi güvenliği kavramı kişisel bilgisayarlardan kurumsal ve ulusal çaptaki tüm bilgi sistemlerine ve kritik altyapılara uzanan geniş bir çerçevede bilgi sistemlerini kapsayan bir güvenlik yönetimi anlayışıdır (The United Nations Economic and Social Commission for Asia and the Pacific [UNESCAP], 2008). Kamu kurumlarının sahip olduğu kurumsal bilgilerin güvenliğini sağlamaları ulusal bilgi güvenliğinin sağlanması noktasında temel teşkil etmektedir. Dolayısıyla kamu kurumlarının bilgi güvenliği kültürü yaklaşımları, yürütmüş oldukları çalışmalar ve bu doğrultuda almış oldukları önlemler ciddi önem arz etmektedir.

Kurumsal bilgiler kurumlar için hayati bir önem taşımaktadır. Kurumsal bilgi, kurumların faaliyetleri ve gereksinimleri doğrultusunda yapılan sistematik araştırma ve geliştirme çalışmalarının sonucu oluşmaktadır (Özdemir, 2019). Kurumların sahip oldukları kurumsal bilgilerini koruyamamasından kaynaklı olarak yaşayacakları sorunlar kurumların büyüklüklerine ve faaliyet alanlarına göre ciddiyetini arttırmaktadır. Kurumsal bilgi kaybı, kurumlar için ciddi maddi ve manevi kayıplara neden olabilmektedir. Bu nedenle kurumların kurumsal bilgilerini korumak için öncelikle sahip olduğu bilgilerin ve bu bilgilerin yer aldığı, oluştuğu, işletildiği ve iletildiği her bilgi varlığının farkında olması gerekmektedir. Kurumsal bilgi varlıklarının belirlenmesi, bu varlıklara ilişkin risk değerlendirme çalışmalarının yapılması, tespit edilen risklere ilişkin etkin bir risk yönetimi süreci işletilmesi kurumsal bilgi güvenliği yönetim sürecini oluşturan önemli adımlardır. Bu süreç gerek sistemler, gerek teknolojik altyapılar, gerek insan gerek ise eğitim gibi birçok farklı faktörün bir araya getirilerek yönetildiği zorlu bir süreçtir. Kurumlar söz konusu çalışmalara başlarken ilk olarak bilgi güvenliğini sağlamaya yönelik yapacakları her türlü faaliyete ilişkin kuralları ortaya koymalı ve dokümante etmelidir. Bilgi güvenliğinin sağlanması amacıyla yapılması gereken çalışmaların planlama, uygulama ve sürekli iyileştirme aşamaları için ihtiyaç duyulan kuralların yazılı olarak hazırlanması gerekmektedir. Bu doğrultuda politika, prosedür, kılavuz, talimat gibi pek çok yol gösterici nitelikteki doküman hazırlanabilmektedir. Bu dokümanların temelini bilgi güvenliği politikası oluşturmaktadır. Bilgi güvenliği politikasında, bilgi güvenliğinin sağlanabilmesi ve belirlenen hedeflerin amacına ulaşabilmesi için yapılması gerekenler ifade edilmektedir. Kurum yönetimi tarafından kurumun amacına uygun ve bilgi güvenliği hedeflerini ortaya koyan nitelikte bir bilgi güvenliği politikası oluşturulmalı ve desteklenmelidir.

Bilgi güvenliğinin sağlanması kapsamında hazırlanan tüm dokümanların amacı; bilgi güvenliğinin üç temel unsuru olan gizlilik, bütünlük ve erişilebilirliğin sağlanarak kurumun sahip olduğu kurumsal bilgilerin güvenliğini sağlamaktır.

Dünyada ve buna paralel olarak ülkemizde bilgi güvenliği yönetim süreçlerine yönelik standart, yasal düzenleme ve diğer ilgili çalışmalar yapılmaktadır. Söz konusu çalışmalar kurumlar için sahip oldukları kurumsal bilgilerinin güvenliğini sağlamaları ve bu kapsamda bilgi güvenliği politika dokümanlarını hazırlama noktasında esas teşkil etmektedir. Bu çalışmaların başında Uluslararası Standardizasyon Örgütü (ISO: International Organization for Standardization) tarafından yayınlanan ve dünya genelinde kabul görmüş bir standart olan ISO 27001 Bilgi Güvenliği Yönetim Sistemi (BGYS) Standardı (Standart) gelmektedir. Standart, bir BGYS kurulması, uygulanması, sürdürülmesi ve sürekli iyileştirilmesi için şartları ortaya koymak amacıyla hazırlanmıştır. Bilgi güvenliği politika dokümanının hazırlanması Standardın öncelikli güvenlik maddelerinin başında gelmektedir.

Ülkemizde Ulaştırma, Denizcilik ve Haberleşme Bakanlığı[1] (UDHB) tarafından 2017 yılında, kamu kurumları arasında veri alışverişlerinde kullanılan web servislerin internet ortamından değil de internet ortamından izole KamuNet (Kamu Sanal Ağı) adı verilen ağ üzerinden sağlanmasına yönelik KamuNet Ağına Bağlanma ve KamuNet Ağının Denetimine İlişkin Usul ve Esaslar Hakkında Tebliğ (Tebliğ) yayınlanmıştır. Tebliğ'de KamuNet'e dahil olmak için asgari gereksinimler belirtilmektedir. Bu gereksinimlerin başında KamuNet'e dahil olacak kamu kurumlarının ISO 27001 uyumlu bir BGYS kurarak tüm süreçler ile ilgili politika ve diğer ilgili dokümanlarını oluşturması ifade edilmektedir.

Ulaştırma ve Altyapı Bakanlığı (UAB) tarafından dönemsel olarak yayınlanan Ulusal Siber Güvenlik Stratejisi ve Eylem Planı'nda (Plan) da kamu kurumlarında BGYS süreçlerinin etkinleştirilmesi ve BGYS'nin yaygınlaştırılmasına yönelik ifadeler yer almaktadır. 2013-2014 Planı "Kamu Bilgi Güvenliği Programı" maddesi kapsamında "bilgi ve iletişim sistemlerinde bulunan güvenlik zafiyetleri, sistemlerin hizmet dışı kalması ve kötüye kullanılmasının engellenebilmesi amacıyla dönemin UDHB koordinasyonuyla Türkiye Bilimsel ve Teknolojik Araştırma Kurumu (TÜBİTAK) Bilişim ve Bilgi Güvenliği İleri Teknolojiler Araştırma Merkezi (BİLGEM) Siber Güvenlik Enstitüsü (SGE) tarafından

[1] Bakanlığın adı, Cumhurbaşkanlığı Hükümet Sistemi ile birlikte "Ulaştırma ve Altyapı Bakanlığı" olarak değiştirilmiştir.

‘Kamu Kurumlarının Uyması Gereken Asgari Bilgi Güvenliği Kriterleri’” dokümanı hazırlanmıştır (TÜBİTAK BİLGEM SGE, 2013). Bilgi güvenliği kriterlerinin yer aldığı dokümanda, tüm kurumlar tarafından bilgi güvenliği politika dokümanının yayınlanması gerektiği açıkça ifade edilmektedir. Kamu kurumlarının uyması gereken asgari bilgi güvenliği kriterleri belirlenirken ISO 27001 ve ISO 27002 standartları temel alınmıştır.

Diğer önemli çalışma ise Cumhurbaşkanlığı Dijital Dönüşüm Ofisi (CB DDO) uhdesinde hazırlanan ve yayınlanan Bilgi ve İletişim Güvenliği Rehberi’dir (Rehber) (Cumhurbaşkanlığı Dijital Dönüşüm Ofisi Başkanlığı [CB DDO], 2020). Söz konusu Rehber, 6 Temmuz 2019 tarihli Cumhurbaşkanlığı Bilgi ve İletişim Güvenliği Tedbirleri Genelgesi (Genelge) uyarınca hazırlanarak Temmuz 2020’de yayınlanmıştır (Cumhurbaşkanlığı, 2019). Genelge’de tüm kurumların Rehber’e uygun hareket etmesi gerektiği vurgulanmıştır. Rehber’de kurumların yürüttükleri BGYS çalışmalarına rehber uygulama sürecinin entegre edilmesi ve yürütülen risk değerlendirme faaliyetlerinde Rehber’de tanımlanan tedbirlerin uygulanması gerektiği ifade edilmektedir. Rehber’de yer alan tedbirlerde, bilgi güvenliği politikası ve bu kapsamda gerekli olan diğer ilgili dokümanların hazırlanması gerektiği ve dokümanlarda asgari olarak nelerin yer alması gerektiği belirtilmektedir.

Kurumsal bilgi güvenliği insan faktörü, eğitim, teknoloji gibi birçok faktörün etki ettiği tek bir çatı altında yönetilmesi zorunlu olan karmaşık süreçlerden oluşmaktadır. Bilgi güvenliği yalnızca bilgi sistemlerinin güvenliğini içermemektedir. Bu nedenle bilginin iyi bir şekilde güvence altına alınması ve etkin bir şekilde yönetilmesi önemlidir (Thakur ve diğerleri, 2016). Bilgi güvenliğine yönelik güvenlik risk ve açıklıkları bilgi sistemlerini yöneten kimselerden kaynaklanabileceği gibi sistemdeki yazılım, donanım, vb. unsurlardan da kaynaklanabilmektedir (Özdemir, 2019). Bilgi sistemlerinin donanım, yazılım, insan faktörü, veriler ve dış ortamın etkileri gibi tüm parçalarının güvenliği göz önünde bulundurulmalıdır (Tvrdikova, 2008). Genel olarak bilgi güvenliğinin sağlanması insan faktörlü etkiler ve bilgi sistemlerinin güvenliği olarak iki ana hususun birlikte değerlendirilmesi olarak ele alınabilmektedir.

Kurumlar tarafından bilgi güvenliği alanında yürütülen faaliyetlerin incelenmesi amacıyla hazırlanan çalışmalara bakıldığında, bilgi güvenliği kapsamına giren ve kurumların bilgi güvenliği politikalarında yer alan temel güvenlik konularından bilhassa eğitim ve farkındalık

faaliyetleri ekseninde insan faktörüne yoğunlaşılarak bilgi güvenliği farkındalığının tespit edilmesine odaklanıldığı görülmektedir. Özdemir (2019) çalışmasında; kamu çalışanlarının bilgi güvenliği farkındalıklarını ortaya koymayı amaçlamış olup bu doğrultuda yürüttüğü çalışmanın sonucunda kamu çalışanlarının orta seviyede bilgi güvenliği farkındalığına sahip olduğunu ifade etmiştir. Kapanoğlu (2016) çalışmasında; öğretmenlerin interneti güvenli kullanım durumlarını ve bilgi güvenliği farkındalık düzeylerini belirlemeyi amaçlamış ve öğretmenlerin bilgi güvenliği farkındalık düzeylerinin orta düzeyde olduğu sonucuna varmıştır. Benzer şekilde Solmaz (2020) çalışmasında, devlet üniversitelerinin eğitim fakültelerinde öğrenim gören öğretmen adaylarının siber güvenlik farkındalık düzeylerini incelemiştir. Araştırmada öğretmen adaylarının siber bilgi güvenliği farkındalıkları ve dijital vatandaşlık düzeylerinin ortalamanın üstünde bir seviyede olduğu sonucuna ulaşılmış ve bilgi ve iletişim teknolojilerinin her alanda kullanıldığı çağımızda gelecek nesilleri yetiştirecek öğretmen adaylarının dijital vatandaşlık düzeyleri ve siber bilgi güvenliği farkındalık seviyelerinin daha da arttırılabilmesi için eğitim fakültelerinde öğretmen adaylarının bu açıdan desteklenmeleri gerektiğini vurgulamıştır. Tuygun (2019) çalışmasında, BGYS sertifikasına sahip olan kamu kurumlarında kurum personelinin sistem hakkındaki düşüncelerini incelemeyi amaçlamıştır. Çalışmanın sonucunda BGYS ekip üyelerinin, ISO 27001 süreçlerinin etkin bir şekilde yönetilebilmesi için gereken teknik yeterlilik, eğitim ve sayısal çokluk noktasında takviye ihtiyaçları olduğu yönünde görüş bildirdiklerini ifade ederken, teknik ekip üyelerinin ise teknik yeterlilikler ve sayısal yeterlilik konusunda görüş birliğinde olmadıklarını ifade etmiştir. Henkoğlu (2015) çalışmasında, Ankara'da bulunan 5 devlet 10 vakıf üniversitesinde hassas bilgi varlıkları ve kişisel verilerin korunmasına ilişkin hususları değerlendirmiştir. Çalışma sonucunda, yasal düzenlemelerin yeterli ve önleyici nitelikte olmadığı, üniversitelerde kişisel verilerin korunmasına yönelik politikaların bulunmadığı, mevcut politika ve kurallar içinde kişisel verilerin korunmasına ilişkin maddelere yer verilmediği ve kişisel verileri işleyen personele veri korumaya ilişkin bilinçlendirme eğitimi verilmediği hususlarını ifade etmiştir. Çek (2017) çalışmasında, iyi ve etkin bir bilgi güvenliği için kurumsal yönetişimin bir parçası olarak bilgi güvenliği yönetişimi kavramından bahsederek kurumlarda bilgi güvenliği yönetişiminin daha etkin hale getirilmesi için yöntem sunmuştur. Çalışma sonucunda, kurumların bilgi güvenliği yönetişimine tüm çalışanların katılım sağlaması ile iyi ve etkin bir bilgi güvenliği yönetişimi olabileceği ifade edilmiş olup bu doğrultuda önerilerde bulunulmuştur. Şişkin (2020) çalışmasında, Ankara'daki üniversite kütüphanelerinin bilgi güvenliği uygulamalarına ve kişisel verilerin korunmasına ilişkin mevcut durumlarını tespit

etmeyi amaçlamış olup çalışma sonucunda, “Üniversite kütüphanelerinde bilgi güvenliği ve kişisel verilerin yönetimine dönük karar verme ve uygulama düzeyindeki eksiklikler (politika, konuyla ilgili bilinç ve farkındalık, risk değerlendirmesi gibi konularda) bulunmaktadır.” hipotezini doğrulamıştır. Vural (2007) çalışmasında, çoğu kurumda güvenlik eğitimleri ve bilinçlendirme programının olmadığını ve olan kurumlarda ise genellikle kullanıcıları bilgi güvenliğinin neden önemli olduğu konusunda eğitmeyi ve bilinçlendirmeyi başaramadığını belirtmiştir.

Literatüre bakıldığında, bilgi güvenliği politikalarında yer alan ağ ve sistem güvenliği, uygulama güvenliği, e-posta güvenliği, parola güvenliği, fiziksel güvenlik gibi temel güvenlik konularının kurumlar tarafından yerine getirilme durumu noktasında yürütülmüş olan çalışmaların ve bu doğrultuda kurumların hazırlamış oldukları bilgi güvenliği politikalarının bütüncül olarak ele alındığı bir çalışmanın bulunmadığı görülmektedir. Ayrıca literatürdeki bazı çalışmalarda da kamu kurumlarının bilgi güvenliği çalışmalarının etkinliği konusunda araştırma yapılması gerekliliğinden bahsedilmektedir.

Tuygun (2019) çalışmasında; kurumsal bilgi güvenliği yönetimlerinin veya bu sistemlerin herhangi bir standardizasyona uyumlu hale getirilmiş olmasının, kurumsal süreçlerde bilgi güvenliğinin tam olarak sağlandığı anlamına gelmediğinin açık olduğu varsayımını yapmış ve kurumsal bilgi güvenliği yönetimlerinin etkinliğinin sorgulanması gerektiğini de vurgulamıştır. Özcan (2009) çalışmasında; kurumsal bilgi güvenliğinin sağlanmasında uygulanan standartların kimi zaman yetersiz kalabileceğini, kurumsal bilgi güvenliği seviyesinin güncel durumunun belirlenmesi amacıyla iç ve dış ortamlardan bağımsız uzman kuruluşlar tarafından denetiminin yapılması gerektiğini, kurumsal bilgi güvenliğinin yönetilmesi zor bir süreç olduğu ve her zaman iyileştirmelere ihtiyaç duyulduğunu belirtmiştir. Çetinkaya (2008) çalışmasında; bilgi güvenliğinin, donanım ve yazılım ile sağlanan çözümlerle sağlanmakta olduğunu fakat bunun etkinliğinin ölçülmediğini ifade etmektedir.

Literatür araştırması sonucundan da anlaşılacağı üzere, kamu kurumlarının bilgi güvenliği politikalarında yer alan temel bilgi güvenliği konularının etkinliğinin bütünsel olarak ele alınarak analiz edilmesi hususunda bir çalışma yapılması gerekliliği bulunmaktadır.

Söz konusu ihtiyaçtan yola çıkılarak bu çalışmada, kamu kurumlarının sahip oldukları bilgilerin güvenliğini sağlamak adına yürütmüş oldukları bilgi güvenliği çalışmalarının ve bu doğrultuda hazırladıkları bilgi güvenliği politikalarının, kurumsal bilgi güvenliğinin sağlanması açısından etkinliğinin ortaya konulması üzerine odaklanılmıştır. Etkinliğin tespit edilmesi için kamu kurumu çalışanları katılımı ile bir anket çalışması gerçekleştirilmiştir.

Anket çalışmasında etkinlik değerlendirilmesi yapılırken, kurumların sahip olduğu verilerin kritiklik düzeyleri ve iş süreçlerinde bilgi sistemleri kullanılma yoğunluğu değişkenleri belirlenmiş ve bu değişkenlere göre sonuçların istatistiksel açıdan anlamlı düzeyde farklılık gösterip göstermeyeceği tespit edilmeye çalışılmıştır.

Problem tanımı

Günümüzde kurumların sahip olduğu kurumsal nitelikteki bilgilerin güvenliğinin sağlanması kurumlar için çok daha önemli hale gelmiştir. Kamu kurumları sahip oldukları bilgilerin güvenliğini sağlamak adına belirli çalışmalar yürütmektedir. Gerek yasal zorunluluk gerekse ihtiyaçtan dolayı bilgi güvenliği yönetim sistemi ve buna temel teşkil eden bilgi güvenliği politikaları birçok kamu kurumu tarafından oluşturulmuş olup buna yönelik çalışmalar sürdürülmektedir. Ancak bu kapsamda yürütülen çalışmaların ve hazırlanan bilgi güvenliği politikalarının kurumsal bilgi güvenliğini sağlama konusunda etkinliği bilinmemektedir. Bu çalışma ile kamu kurumlarında hâlihazırda bulunan bilgi güvenliği politikaları analiz edilerek kurumsal bilgi güvenliğini sağlama konusundaki etkinliği değerlendirilecektir.

Araştırmanın amacı

Bu çalışma ile kamu kurumlarının bilgi güvenliği alanında yürütmüş olduğu çalışmaların, almış olduğu kararların ve hazırlamış olduğu politikaların ulusal bilgi güvenliğinin önemli bir parçası olan kurumsal bilgi güvenliğinin sağlanması açısından etkinliğinin analiz etmek amaçlanmıştır.

Bu temel amaç doğrultusundan oluşturulan araştırma soruları aşağıda belirtilmiştir.

1. Kamu kurumlarının bilgi güvenliği politikalarının etkinliği ile ilgili mevcut durum nedir?

2. Kamu kurumlarının sahip olduğu verilerin kritiklik düzeyi ile sahip oldukları bilgi güvenliği politikalarının etkinliği arasında istatistiksel açıdan anlamlı bir fark bulunmakta mıdır?
3. Kamu kurumlarının iş süreçlerinde bilgi sistemleri kullanım yoğunluğu ile sahip oldukları bilgi güvenliği politikalarının etkinliği arasında istatistiksel açıdan anlamlı bir fark bulunmakta mıdır?

Araştırmanın amacından yola çıkılarak belirlenen yokluk ve varlık hipotezleri aşağıda verilmiştir:

Kurumların sahip olduğu verilerin kritiklik düzeyleri için;

- $H0_a$: Kamu kurumlarının sahip olduğu verilerin kritiklik düzeyi ile bilgi güvenliği politikalarının etkinliği arasında istatistiksel açıdan anlamlı düzeyde bir farklılık bulunmamaktadır.
- $H1_a$: Kamu kurumlarının sahip olduğu verilerin kritiklik düzeyi ile bilgi güvenliği politikalarının etkinliği arasında istatistiksel açıdan anlamlı düzeyde bir farklılık bulunmaktadır.

Kurumların iş süreçlerinde bilgi sistemleri kullanım yoğunluğu için;

- $H0_b$: Kamu kurumlarının iş süreçlerinde bilgi sistemleri kullanım yoğunluğu ile bilgi güvenliği politikalarının etkinliği arasında istatistiksel açıdan anlamlı düzeyde bir farklılık bulunmamaktadır.
- $H1_b$: Kamu kurumlarının iş süreçlerinde bilgi sistemleri kullanım yoğunluğu ile bilgi güvenliği politikalarının etkinliği arasında istatistiksel açıdan anlamlı düzeyde bir farklılık bulunmaktadır.

Araştırmanın önemi

Bu çalışma, yasa koyuculara ve bilgi güvenliği alanında düzenleme ve/veya denetleme yetkisine sahip olan ilgili otoritelere, yürütecekleri çalışmalarda ışık tutması ve ilgili otoritelerce yapılan mevcut düzenlemelerin, atılan adımların ve alınan kararların ne derece yerinde, yeterli ve etkin olduğunun değerlendirilmesinin yapılabilmesi açısından önemlidir. Çalışma ile kamu kurumlarının bilgi güvenliği politikalarında yer alan temel güvenlik

konularına ilişkin kurumların yürütmüş olduğu çalışmaların mevcut durumu tespit edilmeye çalışılmış olup anlamlı farklılıklar oluşturan hususlar ortaya koyularak değerlendirmede bulunulmuştur.

Araştırmadaki varsayımlar

Araştırmada aşağıda belirtilen varsayımlar kabul edilmiştir:

1. Araştırmaya katılan katılımcıların ankete verdikleri yanıtlar katılımcıların gerçek görüşlerini yansıtmaktadır.
2. Araştırmaya örneklemi oluşturan kamu kurumlarının bilgi işlem/bilgi sistemleri birimi çalışanları ve/veya bilgi teknolojileri/güvenliği projelerinde görev alan çalışanlar katılmıştır.
3. Örneklem alınan her bir kamu kurumu evreni yeterince temsil edebilecek durumdadır.

Araştırmanın kapsamı ve sınırlılıkları

Araştırma; araştırma evrenini oluşturan kamu kurumlarından uygun örneklem yöntemiyle seçilen 6 kamu kurumunu kapsamaktadır. Araştırma kapsamındaki kamu kurumlarında anket çalışması uygulanmıştır. 121 katılımcı ankete katılım sağlamıştır. Bu nedenle uygulanan anket çalışması, ankete katılım sağlayanların sayısı ile sınırlıdır.

Tanımlar

- ISO 27001 Bilgi Güvenliği Yönetim Sistemi Standardı: ISO 27001, bilgi güvenliği alanında dünya çapında genel kabul görmüş bir standarttır (Disterer, 2013). İngiliz Standartlar Enstitüsü (BSI: British Standards Institute) tarafından 1995 yılında BS–7799 standardının ilk kısmı olan BS7799–1, 1999 yılında ise aynı standardın ikinci kısmı olan BS7799–2 İngiliz standardı olarak yayınlanmıştır (Vural, 2007). Yıllar içinde standartta birtakım revize çalışmaları yapılmış olup 2005 yılında ISO 27001 adıyla yayınlanmıştır. Standardın 2017 versiyonu güncel olan versiyonudur. Standart, bir BGYS'nin kurulması, uygulanması, sürdürülmesi ve sürekli iyileştirilmesi için şartları ortaya koymak amacıyla hazırlanmıştır (Türk Standardları Enstitüsü [TSE], 2013). Kuruluşlar, Standart kapsamında sertifika alabilmek için bilgi güvenliğinin sağlanmasına yönelik Standart

metninde belirtildiği şekilde BGYS süreçlerini oluşturmaktadır. ISO 27001, kuruluşların bilgi güvenliği hedeflerini bir düzen eşliğinde gerçekleştirmeleri için bir altyapı sunmaktadır. Kuruluşlar, güvenlik gereksinimlerini tutarlı, tekrarlanabilir ve denetlenebilir bir şekilde ele almak için ISO 27001 uygular (Nicho ve Muamaar, 2016). Standart, "Planla - Uygula - Kontrol Et - Önlem Al" (PUKÖ) döngüsünü esas almaktadır. PUKÖ döngüsünde Planla aşaması; BGYS'nin kurulması aşamasıdır. BGYS kapsamının belirlenmesi, amaç ve hedeflerin ortaya konması, süreçlerin, prosedürlerin geliştirilmesi, politikaların oluşturulması, risk analizlerinin yapılıp değerlendirilmesi adımlarını içermektedir. Uygula aşaması; BGYS'nin işletilmesi aşamasıdır. BGYS politikası, kontroller, süreçler ve prosedürlerin gerçekleştirilip işletilmesidir (Marttin ve Pehlivan, 2010). Kontrol et aşaması; BGYS'nin izlenmesi ve gözden geçirilmesi aşamasıdır. İzleme ve gözden geçirme prosedürleri geliştirilmeli ve yürütülmelidir (Kılıç, 2019). BGYS politikalarının, tanımlanmış iş süreçlerinin, alınan önlemlerin değerlendirilmesi; iç tetkik faaliyetlerinin gerçekleştirilmesi ve sonuçların raporlanması adımlarından oluşmaktadır. Önlem al aşaması; BGYS'nin sürekliliğinin sağlanması ve iyileştirilmesi aşamasıdır. Yönetimin gözden geçirme sonuçlarına dayalı olarak, düzeltici ve önleyici faaliyetlerin gerçekleştirilmesidir (Marttin ve Pehlivan, 2010).

- ISO 27002 Bilgi Güvenliği Kontrolleri için Uygulama Prensipleri Standardı:_BGYS uygulamasına ilişkin bir kılavuz ve uygulama rehberi olan ISO 27002, ISO 27001'i tamamlayıcı bir standarttır (Hsu ve diğerleri, 2016). BSI tarafından BS 7799-1 adıyla yayınlanmış olan bu standart, Temmuz 2007'ye kadar ISO 17799:2005 adıyla kullanılmıştır. Temmuz 2007'de ISO 27002:2005 olarak adlandırılmıştır. Yıllar içinde revize çalışmaları yapılarak 2022 yılında güncel halini almıştır. Bu standart, en iyi uygulamaları temel alan bir dizi standarttır ve organizasyonlara bilgi güvenliği programlarını uygularken ve yönetirken uymaları gereken kuralları temin eder (Özbek, 2012). ISO 27001, bilgi güvenliği yönetim sürecini tanımlarken, ISO 27002'de ise ISO 27001'de yer alan önlemlerin detaylı açıklamaları ve uygulamaları yer almaktadır (Özbilen ve Çağlar, 2020).
- Ulusal Siber Güvenlik Stratejisi ve Eylem Planı: 28447 sayılı "Ulusal Siber Güvenlik Çalışmalarının Yürütülmesi, Yönetilmesi ve Koordinasyonuna İlişkin Karar" gereğince ulusal siber güvenliğin sağlanması için politika, strateji ve eylem planlarını hazırlama görevi dönemin UDHB'ye verilmiştir (Bakanlar Kurulu, 2012). Plan, 2013-2014, 2016-2019 ve 2020-2023 yıllarını kapsayacak şekilde dönemsel olarak hazırlanmaktadır. Yayınlanan her yeni strateji, bir önceki dönemde hayata geçirilen stratejilerde elde edilen

kazanımları bir üst seviyeye taşımayı amaçlamaktadır. Siber tehditlerde ortaya çıkan eğilimler, teknolojik gelişmeler, ulusal beklentiler ve uluslararası uygulamalar dikkate alınarak strateji hedefleri belirlenmektedir. 2020-2023 Planı'nın ilk eylem maddesi olan "Siber Güvenlik Düzenlemelerinin Gerçekleştirilmesi ve Denetimlerin Yapılması" başlığı altında tanımlanan uygulama adımlarından dördüncü uygulama adımında "Kamu kurumlarınca BGYS'nin uygulanmasının yaygınlaştırılması" hususu ifade edilmiştir. Uygulama adımının ölçüm kriteri olarak "ISO 27001'e uyum belgesi alan kamu kurumu sayısının artırılması" kriteri belirlenmiştir.

- Kamu Kurumlarının Uyması Gereken Asgari Bilgi Güvenliği Kriterleri: "Kamu Kurumlarının Uyması Gereken Asgari Bilgi Güvenliği Kriterleri" (Asgari BG Kriterleri) dokümanı, "Ulusal Siber Güvenlik Stratejisi ve 2013-2014 Eylem Planı"nın (Ulaştırma, Denizcilik ve Haberleşme Bakanlığı [UDHB], 2013) 6'ncı ana eylem maddesi olan "Kamu Bilgi Güvenliği Programı" kapsamında UDHB koordinasyonuyla TÜBİTAK BİLGEM SGE tarafından hazırlanmıştır (TÜBİTAK BİLGEM SGE, 2013). Dokümanda yer alan kriterler ülkemizdeki tüm kamu kurumlarını kapsamaktadır. Öncelikli olarak kritik bilgi sistemi bulunan ve bulunmayan kurumlar olarak kamu kurumları sınıflara ayrılmıştır. Bu kapsamda kamu kurumları tarafından alınması gereken bilgi güvenliği kriterleri belirlenmiştir. Dokümanda bahsedilen ve tüm kamu kurumlarının alması gereken asgari bilgi güvenliği kriterlerinin başında bilgi güvenliği politika dokümanlarının hazırlanması gelmektedir.
- KamuNet Ağına Bağlanma ve KamuNet Ağının Denetimine İlişkin Usul ve Esaslar Hakkında Tebliğ: KamuNet; kamu kurum ve kuruluşları tarafından özel ağ ile internet ortamından yalıtılmış şekilde hizmet, işlem ve veri trafiğinin aktarılacağı, fiziksel ve siber saldırılara karşı daha güvenli kapalı devre, kamu sanal ağı altyapısıdır (UDHB, 2017). KamuNet ağına dâhil olunması amacıyla "Kamu Kurum ve Kuruluşlarının KamuNet'e Dahil Edilmesi ile İlgili 2016/28 Sayılı Başbakanlık Genelgesi", 03.12.2016 tarih ve 29907 sayılı Resmi Gazete'de yayımlanarak yürürlüğe girmiştir (Başbakanlık, 2016). KamuNet projesi ile kamu kurum ve kuruluşları arasındaki veri iletişiminin internete kapalı, fiziksel ve siber saldırılara karşı daha güvenli sanal bir ağ üzerinden yapılması; siber güvenlik risklerinin minimize edilmesi, mevcut ve kurulacak olan güvenli kapalı devre çözümlere standart sağlanması, ortak uygulamalar için uygun alt yapının tesis edilmesi amaçlanmaktadır (UDHB, 2015). 2017 yılında KamuNet'e dahil olacak kamu kurum ve kuruluşları için KamuNet'e bağlanma ve bu KamuNet'in denetimi için usul ve esasların yer aldığı düzenleme yapılmıştır. Kamu kurumlarının birbirleriyle güvenli

iletişim sağladıkları KamuNet'e ilişkin 21.06.2017 tarih ve 30103 sayılı Resmi Gazete'de "KamuNet Ağına Bağlanma ve KamuNet Ağının Denetimine İlişkin Usul ve Esaslar Hakkında Tebliğ" yayınlanarak yürürlüğe girmiştir (UDHB, 2017). Tebliğin, kamu kurumu yükümlülükleri ve asgari gereksinimlerin yer aldığı ikinci bölümü 4. maddesi a bendi uyarınca KamuNet bağlantısı yapacak tüm kamu kurumlarının birimleri ve sistemlerini kapsayacak şekilde BGYS kurmasını ve işletmesini zorunlu kılınmıştır (Tuygun, 2019). Bu bağlamda KamuNet'e dahil olacak kamu kurumları ISO 27001 uyumlu BGYS kurma ve bu kapsamdaki faaliyetlerinin ISO 27001'e uyumluluğunu belgelendirmek adına çalışmalar yürütmektedir. Bu çalışmalar kapsamında da kurumlar, temel olarak bilgi güvenliği politika dokümanlarını oluşturmaktadır.

- Bilgi ve İletişim Güvenliği Tedbirleri Genelgesi: 2019 yılında tüm kamu kurum ve kuruluşları ve kritik altyapı işletmeleri için asgari olarak uyulması gereken bilgi ve iletişim güvenliği tedbirlerini ele alan düzenleme hazırlanmıştır. 06.07.2019 tarih ve 30823 sayılı Resmi Gazete'de Bilgi ve İletişim Güvenliği Tedbirleri konulu 2019/12 sayılı Cumhurbaşkanlığı Genelgesi yayımlanmıştır (Cumhurbaşkanlığı, 2019). Genelge'de bilgi sistemleri ortamında bulunan milli güvenliği tehdit edecek kritik düzeydeki bilgilerin gizliliğinin, bütünlüğünün ve erişilebilirliğinin sağlanmasına yönelik alınabilecek en temel tedbirlerden bahsedilmektedir. Tüm kamu kurum kuruluşları ve kritik altyapı işletmelerinin yeni kurulacak bilgi sistemlerinin Genelge kapsamında hazırlanması öngörülen Rehber'de ifade edilen hususlara uygun olarak oluşturulması ve halihazırda bulunan sistemlerini kademeli olarak söz konusu Rehber'e uygun hale getirilmesi gerektiği ifade edilmektedir.
- Bilgi ve İletişim Güvenliği Rehberi: 06.07.2019 tarih ve 2019/12 sayılı Cumhurbaşkanlığı Genelgesi uyarınca CB DDO tarafından hazırlanan "Bilgi ve İletişim Güvenliği Rehberi", 24 Temmuz 2020 tarihinde yayınlanmıştır. Rehber, bilgi ve iletişim güvenliği alanında ülkemize özgün ilk referans doküman olma niteliği taşımaktadır (CB DDO, 2020). Rehber'de yer alan tedbirlere, tüm kamu kurum kuruluşları ve kritik altyapı işletmelerinin yeni kurulacak ve halihazırda bulunan bilgi sistemlerinin uyması zorunludur. Kurumlar Rehber'de belirtilen güvenlik seviyelerine göre, mevcut bilgi sistemlerini Rehber'de yer alan yol haritasına uygun olarak kademeli olarak tedbirlere uyumlu hale getirecektir. Bilgi ve iletişim güvenliği alanında ulusal bir dönüşümün temel taşı olarak tasarlanmıştır (Klynveld Peat Marwick Goerdeler [KPMG], 2020). Rehber'de ihtiyaçlar, gelişen teknoloji ve değişen şartlar göz önünde bulundurularak Rehber'in güncelleneceği bu bakımdan yaşayan bir doküman niteliğinde olduğu ifade edilmektedir. Rehber'de, 15

alan ve 62 ana başlık altında sınıflandırılmış olan toplam 659 tedbir ve denetim maddesine uyulması zorunlu kılınmıştır (Gözel, 2020). Rehber'de kurumların rehber uygulama sürecini, yürüttükleri BGYS'ye entegre etmesi gerektiği ve bilgi güvenliği risk yönetimi faaliyetleri kapsamında rehberde tanımlanan tedbirleri uygulaması gerektiği anlatılmaktadır. Rehber uyum çalışmaları kapsamında kurumlar, sahip oldukları bilgi varlıklarını belirleme, bilgi varlıklarının kritiklik derecelerini tespit etme ve bu doğrultuda tedbir almaya yönelik çalışmalarını sürdürmektedir. Rehber'de yer alan tedbirlere ilişkin kurumlar tarafından politika ve diğer ilgili dokümanların oluşturulması gerektiği de ifade edilmektedir.

- Bilgi Güvenliği Yönetimi Rehberi: TÜBİTAK BİLGEM Yazılım Teknolojileri Araştırma Enstitüsü (YTE) tarafından hazırlanan "Bilgi Güvenliği Yönetimi Rehberi" (BGYR) Ocak 2021'de yayınlanmıştır (TÜBİTAK BİLGEM YTE, 2021). TÜBİTAK BİLGEM YTE "Dijital Olgunluk Modeli" kapsamında yer alan yetkinlikler ve söz konusu yetkinlikler kapsamında yer alan dijital kabiliyetler dikkate alınarak yol gösterici olarak kullanılmak üzere öncelikle "İşletim ve Bakım Yetkinliği"ne ilişkin olarak "İşletim ve Bakım Rehberi" hazırlanmış ve 2017 yılında yayınlanmıştır (TÜBİTAK BİLGEM YTE, 2017). "İşletim ve Bakım Yetkinliği" altında hazırlanan rehberlerden birisi de BGYR'dir. BGYR, BGYS'nin kurulumu ve işletilmesi sırasında yapılması veya gözden geçirilmesi gereken hususlar ve uygulanması gereken faaliyetler konusunda kurumlara yol gösterici nitelikte bir dokümandır. BGYR'de, kamu kurumlarında bilgi teknolojileri yönetim standartlarına uyum konusunda ciddi bir açık olduğu bu nedenle söz konusu rehberin kamu kurumlarına önemli bir katkı sağlayacağının öngörüldüğü ifade edilmektedir. BGYS kapsamında hazırlanan bütün bilgi güvenliği politikalarına altyapı oluşturan temel bir bilgi güvenliği politikasının oluşturulması gerektiği de vurgulanmıştır.

2. KAVRAMSAL ÇERÇEVE

Araştırma, bilgi güvenliği kavramından hareketle bilgi güvenliği ve kurumsal bilgi güvenliği kavramlarına öncelik vermekte ve kurumsal bilgi güvenliğinin önemine değinerek kurumsal bilgi güvenliğinin sağlanmasına yönelik politikaları, bu kavramlar üzerinden incelemeye çalışmaktadır.

2.1. Bilgi Güvenliği ve Unsurları

Bilgi, modern toplumda kilit bir unsurdur. Bilgi ve bilişim güvenliği konusuna gelindiğinde ise günümüzde en değerli güç unsurlarının başında geldiğini söylemek olanaklıdır (Özbilen ve Çağlar, 2020). Bu nedenle bilginin iyi bir şekilde güvence altına alınması ve etkin bir şekilde yönetilmesi önemlidir (Thakur ve diğerleri, 2016). Daha önceleri genellikle fiziksel ortamlarda tutulan bilgi, günümüzde dijital ortamlara da taşınmıştır. Fiziksel ortamlarda tutulan bilginin korunması için fiziksel önlemlerin alınması yeterli olabilecekken, dijital ortamlarda muhafaza edilen bilginin korunması için fiziksel önlemlerin yanı sıra daha farklı önlemlerin de alınması gerekmektedir.

Bilginin fiziksel ortamlardan dijital ortamlara geçmesi ile bilginin korunmasının yanı sıra günümüzde bilgi güvenliği kavramı önemli hale gelmiştir. Bilgi güvenliği bilginin korunduğu ve saklandığı bilgi sistemlerinin ve sistemin içerdiği bilginin yetkisiz erişimine, kullanımına, ifşa edilmesine, değiştirilmesine, incelenmesine, hasar verilmesine veya yok edilmesine karşı korunması ve buna ilişkin tedbirlerin bütünü olarak tanımlanabilir. Kişisel bilgisayarlardan kurumsal ve ulusal çaptaki tüm bilgi sistemlerine ve kritik altyapılara uzanan geniş bir çerçevede bilgi sistemlerini kapsayan bir güvenlik yönetimi anlayışıdır (UNESCAP, 2008). Güvenlik, bilgi sistemi tasarımı ve geliştirilmesinin önemli bir parçasıdır. Bilgi sistemleri güvenliği sadece bilgi teknolojileri güvenliğinin yönetimi ile çözülemez çünkü bilgi teknolojileri bilgi sistemlerinin sadece bir parçasını oluşturmaktadır. Bilgi sistemlerinin donanım, yazılım, insan faktörü, veriler ve dış ortamın etkileri gibi tüm parçalarının güvenliği göz önünde bulundurulmalıdır (Tvrdikova, 2008).

Bilgi güvenliği unsurları genel kabul görmüş haliyle gizlilik, bütünlük ve erişilebilirlik diğer bir ifadeyle kullanılabilirlik olarak değerlendirilmektedir.

Gizlilik; önemli ve hassas bilgilerin istenmeyen biçimde yetkisiz kişilerin eline geçmesi önlenmesi ve sadece erişim yetkisi verilmiş kişilerce erişilebilir olduğu garanti altına alınması, bütünlük; bilginin bir kısmının veya tümünün yetkili olmayan kişilerce değiştirilmesinin, silinmesinin ve bozulmasının önlenmesi, erişilebilirlik; bilgi veya bilgi sistemlerinin sürekli kullanıma hazır ve erişilebilir olması şeklinde tanımlanmaktadır (Ersoy, 2012). Bunlar genel kabul görmüş bilgi güvenliği unsurları olarak değerlendirilirken, bazı çalışmalarda bu unsurlara destek olan ilkelerden de bahsedilmektedir. Örneğin bir çalışmada (Canbek ve Sağıroğlu, 2006), belirli bir eylemin gerçekleştirilmesinden kimin ya da neyin sorumlu olduğunun belirlenmesi olarak sorumluluk ilkesinin bilgi güvenliğine katkı sağlayan bir ilke olduğundan bahsedilmektedir. Bilgi güvenliğinin göz önünde bulundurulması gereken diğer ilkeleri ise kayıt altına alma, kimlik tespiti, güvenirlik ve inkâr edememe (sayısal imza yöntemiyle gönderici ve alıcı arasındaki işlemler) şeklinde sıralanabilir (Tekerek, 2008).

Söz konusu unsurlar ve temel ilkeler çerçevesinde gerek ulusal gerek uluslararası düzeyde bilgi güvenliğine dair politika araçları geliştirilmekte ve çeşitli politika önerileri hayata geçirilmektedir.

2.2. Kurumsal Bilgi Güvenliği ve Önemi

Bilgi kurumun diğer önemli varlıkları gibi kurum için değeri olan ve bu nedenle uygun olarak korunması gereken varlıktır. Günümüzde kurum ve kuruluşların değeri, sahip oldukları bilgi ile ölçülmektedir. Kurumlar için bilgi bu denli önemli bir hal almışken bilginin bulunduğu her ortamın korunması ve güvenliğinin sağlanması gerekmektedir.

Günümüzde hızla gelişen bilişim teknolojileri, bilginin iletilmesinde, saklanmasında ve paylaşılmasında sağladığı olanaklar ile hem kişisel kullanıcılara, hem de kurumlara çok büyük fayda ve avantajlar sağlamaktadır (Acılar, 2009). Bilgi ve iletişim teknolojilerindeki gelişmeler, vatandaşların bilgiye olan taleplerini artırmakta ve bu durum kamu kuruluşlarını yeni arayışlara ve yöntemlere sevk etmektedir (Kırışık ve Sezer, 2015). Bu nedenle kurumların iş süreçlerini gerçekleştirirken bilişim teknolojilerini kullanmaları kaçınılmaz olmaktadır. Kurumlar için bilgi güvenliğinin sağlanması adına fiziksel güvenlik önlemlerinin alınmasının yanı sıra bilişim teknolojilerini kullanmanın neden olabileceği bilgi güvenliği risklerine yönelik de önlem alınması gerekliliği doğmaktadır. Kurumun bilgi

işlem sistemine yapılacak bir saldırı ciddi miktarda para, zaman, itibar ve değerli bilgi kaybına sebep olabilmektedir (Dayıoğlu, 2002). Kurumlar sahip oldukları bilişim teknolojilerinin yaşanabilecek saldırılara karşı korunaklı hale gelmesi adına önlemler almaktadır. Bir bilgi güvenliği olayının meydana gelmesi, verilen hizmetlerin seviyesini düşürebilmektedir veya hizmetlerin kullanılabilir olmamasına neden olabilmektedir (Szczepaniuk ve diğerleri, 2020).

Bilişim teknolojileri güvenliği içerisine, donanım, yazılım, bilgi ve iletişimi kapsayan bilgi sistemlerinin gizlilik, güvenlik, bütünlük ve her zaman çalışır vaziyette olmasının sağlanması girmektedir (Onwubıko ve Lenaghan, 2007). Sadece teknik önlemlerle (güvenlik duvarları, atak tespit sistemleri, antivirüs yazılımları, anticasus yazılımlar, şifreleme, vb.) bilgi güvenliğinin sağlanması mümkün değildir (Vural, 2007). Kurumsal bilgi güvenliği insan faktörü, eğitim, teknoloji gibi birçok faktörün etki ettiği tek bir çatı altında yönetilmesi zorunlu olan karmaşık süreçlerden oluşmaktadır. Bilgi güvenliğinin sağlanması yalnızca bilgi teknolojileri birimine ait bir iş olarak görülmemelidir. Oysa ki bilgi güvenliği; teknoloji, süreç ve insan faktörlerinin beraber değerlendirilmesi gereken ve bu üç faktöre göre oluşturulması gereken bir kavramdır (Çek, 2017).

Bu nedenle de kurumsal bilgi güvenliği kültürünün oluşturulması önemlidir. Çoğu bilgi güvenliği tedbiri, teknik düzeyde olup, bilgi güvenliği yönetimi güvenlikle ilgili teknik çalışanlara bırakılmış olsa da bilgi güvenliği ağırlıklı olarak yönetimi ilgilendiren bir konudur (Woodhouse, 2007). Yönetimin bu konudaki destekleyici tutum ve davranışları ve çalışanların özverileri ile bilgi güvenliği kültürü oluşmakta olup bu sayede bilgi güvenliği çalışmaları amacına ulaşabilmektedir. Bir kurumda çalışanların güvenlik gerekliliklerini karşılamadığı durumda, bilgi güvenliği politikasının uygulanması başarısız olabilmektedir (Angraini ve diğerleri, 2019).

Kurumsal bilgi güvenliğini sağlamadaki temel amaç; veri bütünlüğünün korunması, yetkisiz erişimin engellenmesi, mahremiyet ve gizliliğin korunması ve sistemin devamlılığının sağlanmasıdır. Kurumsal bilgi güvenliği, bilginin üretildiği, işlendiği ve saklandığı her ortamda sağlanmak zorundadır. Bunun için mevcut yazılımlar, donanımlar, ortamlar ve insan kaynakları dikkate alınmalıdır (Vural ve Sağıroğlu, 2008). Kurumsal bilgi güvenliğinin sağlanması için kurumların bilgi varlıklarını tespit ederek zafiyetlerini belirlemesi ve istenmeyen tehdit ve tehlikelerden korunmak amacıyla gerekli güvenlik

analizlerinin yapılarak önlemlerin alınması gerekmektedir. Kurumlar, yetersiz bilgi güvenliği politikaları nedeniyle bu tür istenmeyen tehdit ve tehlikelerin kurbanı olabilmektedir (Alqahtani, 2017).

2.3. Bilgi Güvenliği Politikaları

Politika bir kurallar bütünüdür ve sistemin davranış şeklini belirten bir durumdur (Can ve Ünalır, 2010). Bilgi güvenliği politikası ise bilgi varlıklarının nasıl kullanılması gerektiğine ilişkin kurallar bütünüdür. Bilgi güvenliğinin temel unsurlarından hareketle ihtiyaç duyulan çok çeşitli alanlarda politika geliştirilmesi ihtiyacı kaçınılmazdır. Birbirine bağlı bilgi sistemleri ve ağlar, kurum ve kuruluşları sahip oldukları bilgilerin korunması için belirgin önlemler alınması gerektiği ihtiyacı gibi önemli bir duruma itmektedir. "Güvenlik kültürü" iş rekabetinin çok önemli bir parçası haline gelmiştir ve güvenlik politikası iş yönetiminin önemli bir bileşenidir (Luma ve Abazi, 2019). Kurum ve kuruluşlar, işleyişleri ve refahı için hayati önem taşıyan çok miktarda bilgi üretir, kullanır, saklar ve iletir. Bilgilerin gerektiğinde gizli tutulması, gerektiğinde ve gerektiğinde erişilebilir olması ve değişiklik ve bütünlük kaybından korunması gereklidir. Kurum ve kuruluşların bilgi ve teknoloji kullanıcılarının standartlarını, sınırlarını ve sorumluluklarını tanımlayan bir bilgi güvenliği politikası oluşturması; bilgi ihlallerine yönelik tehditleri ele almak için temel bir yaklaşımdır (Bhaharin ve diğerleri, 2019). Bilgi güvenliği politikası; bilginin gizliliğini, bütünlüğünü ve erişilebilirliğini korumak amacıyla oluşturulmuş kontrollerin uygulanması sırasında uyulması gereken prensiplerin belirtildiği dokümandır. Güvenlik politikaları kurum veya kuruluşlarda kabul edilebilir güvenlik seviyesinin tanımlanmasına yardım eden, tüm çalışanların ve ortak çalışma içerisinde bulunan diğer kurum ve kuruluşların uyması gereken kurallar bütünüdür (Kalman, 2003). Bilgi güvenliği politikasında ve bu kapsamda oluşturulan ilgili dokümanlarda, kurum tarafından belirlenen hangi eylemin onaylanmış veya onaylanmamış olduğu yazılı hale getirilmektedir. Her kurum ve kuruluşun yapısı farklı olduğu için doğası gereği güvenlik politikaları farklılık göstermektedir. Ancak kurumsal bilgi güvenliği politikaları, genellikle çalışanın sorumluluklarını, güvenlik denetim araçlarını, amaç ve hedeflerini kurumsal bilgi varlıklarının yönetimini, korunmasını, dağıtımını ve önemli işlevlerin korunmasını düzenleyen kurallar ve uygulamaların açıklandığı genel ifadeleri içermektedir.

Bilgi güvenliği politikalarının temel amacı; çalışanların ve ilgili tarafların uyması gereken bilgi güvenliği şartlarının çerçevesini çizmek ve yazılı kuralları belirlemektir. Bilgi güvenliği politikalarının diğer alt amaçları ise her kurum kendi çalışanlarının bilgi güvenliği farkındalık seviyesini artırmak, bilgi güvenliği teknik ve idari tedbirlerini almak, ilgili taraflarla yapılacak anlaşmalar için gizlilik hükümlerini belirlemek, kurum itibarını korumak, kurumun ana ve destekleyici iş faaliyet en az kesinti ile devam etmesini sağlamak ve çalışanlarının bilgi güvenliği gereksinimlerine uygun şekilde hareket etmesi konusunda yol gösterici olmaktır. Bunun yanı sıra bilgi güvenliği politikalarının kurumlara getirdiği birtakım faydalar da bulunmaktadır. Can ve Akbaş (2014) çalışmalarında bilgi güvenliği politikalarının kurum çalışanlarını ve üçüncü tarafları yasal sorumluluktan kurtardığı, kuruma ait gizli bilgilerin, yetkisiz kişilerin eline geçmesi, ortaya çıkarılması ve değiştirilmesi durumlarına karşı kurumu koruduğu ve kurumun bilişim kaynaklarının boşa kullanımının ve israfının engellediğini ifade etmektedir.

Kurumlar iş süreçleri ve ihtiyaçları doğrultusunda kurum yapısına uygun olarak güvenlik politikalarını oluşturmalı ve üst yönetimin bu konudaki desteğini almalıdır. Üst yönetimin desteği, kurumda bilgi güvenliğinin sağlanmasında gereken kararlılığının gösterileceğini ifade etmekte ve kurum çalışanlarının bilgi güvenliğine daha çok önem vermesini sağlamaktadır (Öztürk, 2008). Bilgi güvenliğine yönelik yapılan çalışmaların amacına ulaşabilmesinde üst yönetimin destekleyici tutum ve davranışları önem arz etmektedir. Bilgi güvenliği politikası temel politika niteliğinde hazırlanmalıdır. Diğer güvenlik politikaları temel bilgi güvenliği politikasına uyumlu olmalı ve ondan beslenmelidir (TÜBİTAK BİLGEM YTE, 2021).

Alshaikh ve diğerleri (2015) çalışmalarında bilgi güvenliği politika geliştirme modeli ortaya koymuştur. Önerilen model geliştirme, uygulama ve bakım ve değerlendirme aşamalarından oluşmaktadır. Her aşama yapılması gereken adımları anlatmaktadır. Politika geliştirme aşaması temel olarak politika geliştirme ekibinin kurulması, kurum dış paydaşlarının belirlenmesi, rol ve sorumluluk atamaları adımlarından oluşmaktadır. Temel adımları takiben kurumun güvenlik gereksinimlerinin belirlenmesi, mevcut güvenlik politika ve prosedürlerinin değerlendirilmesi, politika bileşenlerinin belirlenerek taslak politika dokümanının oluşturulması ve gözden geçirilmesi adımları yer almaktadır. Önerilen modelde geliştirilen bilgi güvenliği politikasının uygulama ve bakım aşamasında, politikanın çalışanlara ve dış paydaşlara duyurulması, hangi kanallardan erişilebileceğinin belirlenmesi,

politika hakkında yeterli farkındalığın sağlanması ve politikanın uygulanması için gerekli faaliyetlerin yürütülmesi adımları ifade edilmektedir. Politikanın son aşaması olan değerlendirme aşamasında ise politikanın güncelliğinin sağlanması adına düzenli aralıklarla gözden geçirilmesi, politika hakkında çalışanlar ve dış paydaşlardan geri bildirim alınması, politikanın bu doğrultuda olgunlaştırılması ve bilgi güvenliği olaylarının değerlendirilmesi ve risk değerlendirme yaklaşımının gözden geçirilmesi adımlarından bahsedilmektedir.

Bilgi güvenliği politikalarının oluşturulması ve politikaların uygulamaya dönüşmesi aşamasında, tüm yönleri ile birlikte değerlendirme yapılmadığı müddetçe, bilgi güvenliğinin sağlanmasında başarıya ulaşılması söz konusu değildir (Henkoğlu ve Yılmaz, 2013).

Bilgi güvenliği politikası açık ve anlaşılır bir dille yazılmalıdır. Kurum çalışanları ve dış paydaşlar tarafından net bir şekilde anlaşılabilir olması ve gizli nitelikte bilgilere politika dokümanında yer verilmemesi gerekmektedir. İyi bir güvenlik politikası, kullanıcıların isini zorlaştırmamalı, kullanıcılar arasında tepkiye yol açmamalı, kullanıcılar tarafından uygulanabilir olmalıdır (Vural, 2007).

Bilgi güvenliği politika dokümanı temel olarak aşağıda belirtilen başlıklara sahip olmalıdır (InstantSecurityPolicy, 2010):

- Genel Açıklama: Politikanın ele alacağı konu hakkında temel bilgi sağlar.
- Amaç: Politikaya neden ihtiyaç duyulduğunu belirtir.
- Kapsam: Politikanın neleri ve kimleri içine aldığını belirtir.
- Hedef Kitle: Politika kapsamında belirtilen esaslara uyulması amacıyla ilgili tavsiyeleri ve bildirimleri içerir.
- Politikalar: Politika dokümanının ana kısmını oluşturan ve uyulması gereken esasları maddeler halinde ifade eden kurallardır.
- Tanımlar: Teknik terimlerin açıklandığı tanımlar bölümüdür.
- Versiyon: Politika dokümanının güncellenmesi gerektiği durumlarda ilgili değişiklerin yansıtılabilmesi için doküman versiyon numarasıdır.

Temel bilgi güvenliği politikası ile uyumlu olarak belirli bir konu özelinde oluşturulmuş ve konu ile ilgili detaylı bilgiler içeren diğer politika dokümanları da oluşturularak ana çatıyı oluşturan bilgi güvenliği politikası desteklenmelidir. Kurumların farklı yapılarda olması

gereği ile bu doğrultuda hazırlanabilecek ilgili destekleyici politikalar kurum özelinde değişiklik gösterebilmektedir. Çizelge 2.1'de kurumlar tarafından hazırlanabilecek destekleyici politikalar açıklamaları ile verilmektedir.

Çizelge 2.1. Hazırlanabilecek destekleyici politikalar ve açıklamaları

Politika Adı	Açıklama
E-posta Kullanım Politikası	E-postaların doğru kullanımı için kurallar tanımlayan politikadır. Çalışanların e-posta kullanırken dikkat etmesi gereken hususları içermektedir.
Parola Politikası	Parola yönetimi için kurallar tanımlayan politikadır. Parolaların güvenliğinin sağlanması ve güçlü parola oluşturulması için dikkat edilmesi gereken hususları içermektedir.
Erişim Kontrol Politikası	Çalışanların ağ ve hizmetlere, sistemlere, uygulamalara ve bilgi varlıklarına erişimlerine ilişkin kurallar tanımlayan politikadır. Ayrıcalıklı erişim haklarının yönetimi, gizli kimlik bilgilerinin yönetimi, kullanıcı erişim haklarının yönetimi ve gözden geçirilmesi, ağ ve hizmetlere erişim, sistem ve uygulamalara erişim gibi konuları içermektedir. Erişim kontrol politikasının hedefi doğru kişinin, doğru bilgiye doğru zamanda ulaşmasıdır (Aktaş, 2020).
Uzaktan Erişim ve Çalışma Politikası	Kurum hizmetlerine ve bilgi varlıklarına uzaktan erişim ve çalışma gerektiği durumlarda çalışanların uyması gereken kuralları tanımlayan politikadır. Uzaktan erişim yönteminin nasıl olacağı ve dikkat edilmesi gereken konuları içermektedir.
İnternet Kullanım Politikası	Çalışanların internet kullanımına ilişkin uyması gereken kuralları tanımlayan politikadır. İnternet hizmetinin uygun olmayan kullanımının önüne geçmek, internet güvenliğini sağlamak, yasal yükümlülüklere uyum sağlamak adına dikkat edilmesi gereken konuları içermektedir.
Mobil Cihaz Kullanım Politikası	Mobil cihazların kullanımına yönelik kurallar tanımlayan politikadır. Taşınabilir veri depolama ortamları, dizüstü bilgisayarlar, akıllı telefon, tablet gibi üzerinde bilgi barındıran cihazların güvenli kullanım esaslarını içermektedir.
Kabul Edilebilir Kullanım Politikası	Çalışanların kurum varlıklarını kullanırken uyması gereken kuralları tanımlayan politikadır. Son kullanıcı politikaları olarak da ifade edilebilmektedir. Kabul edilebilir kullanım politikası, kurum bilgi ve iletişim varlıklarının iş amaçlarına uygun kullanılması için gerekli kuralları belirler (Eskiyörük, 2008).
Tedarikçi İlişkileri Güvenliği Politikası	Tedarikçiler tarafından temin edilen mal veya yerine getirilen hizmetlerin sağlanmasında bilgi güvenliği gereksinimlerinin karşılanması amacıyla tedarikçilerin uyması gereken kuralları tanımlayan politikadır.

Çizelge 2.1. (devam) Hazırlanabilecek destekleyici politikalar ve açıklamaları

Fiziksel ve Çevresel Güvenlik Politikası	Kurumların karşı karşıya kalabileceği fiziksel ve çevresel güvenlik ihlallerini önlemek amacıyla uyulması gereken kuralları tanımlayan politikadır. Çalışma odalarının güvenliği, sistem odası, kritik bilgi işleme yerleri gibi alanların fiziksel (güvenli giriş-çıkış kontrolleri, fiziki kontroller vb.) ve çevresel (yangın, sel, deprem vb. çevresel tehditlere yönelik kontroller) güvenliğini sağlamaya yönelik kuralları içerir.
Temiz Masa Temiz Ekran Politikası	Çalışma esnasında veya dışında; kurum varlıklarını korumaya yönelik çalışma masalarında, ofis ve odalarda, bilgisayar ekranı ve diğer donanımların kullanımında uyulması gereken kuralları tanımlayan politikadır. Çalışma esnasında veya dışında bilginin zarar görmesi riskini azaltmaya yönelik kuralları kapsamaktadır.
Yedekleme ve İş Sürekliliği Yönetimi Politikası	Sel, deprem, yangın gibi çevresel tehditler, sistem ve donanım arızaları, insan kaynaklı hatalar gibi durumların yaşanma ihtimaline karşı yapılması gerekenlere ilişkin kuralları tanımlayan politikadır. Yedekleme sistemi, yedeklenecek veri miktarı, yedekleme sıklığı, iş sürekliliği planı, olası senaryolar, tatbikat ve test süreçleri gibi hususları içermektedir.
Risk Yönetimi Politikası	Risklerin tespit edilmesi, değerlendirilmesi ve işlenerek kabul edilebilir seviyeye düşürmek veya tamamen ortadan kaldırmak için yapılması gereken hususları tanımlayan politikadır. Bilgi güvenliği risk yönetimi, risklerin kurumun hedeflerine ulaşabilmek için her seviyede risklerini belirli bir yöntemle sistematik olarak tespit etmesi, değerlendirmesi, risklerin etkilerini azaltmak için önlemler alması ve bu sürecin etkin işlemesini sağlayacak şekilde izlenmesidir (Altınpulluk, 2016).
İhlal Olay Yönetimi Politikası	Bilgi güvenliği ihlal olaylarının tespit edilmesi ve yönetilmesinde izlenecek adımları tanımlayan politikadır. İhlal olaylarının bildirilmesi, süreçte yer alan kişilerin sorumlulukları, olayların raporlanması ve değerlendirilmesi gibi ihlal olaylarının tespiti ve yönetilmesine ilişkin kuralları kapsamaktadır.
Bilgi Sınıflandırma ve Etiketleme Politikası	Bilginin önem derecesine göre sınıflandırılması ve sınıflandırma düzeyine uygun şekilde etiketlenmesi ve bu doğrultuda güvenlik önlemlerinin alınması için gereken kuralları tanımlayan politikadır. Amaç varlıklar için uygun korumanın sağlanması ve Bilgi kaynaklarının uygun koruma seviyesine sahip olduklarının garanti edilmesidir (Vural, 2007).
Ağ ve Sistem Güvenliği Politikası	Ağ ve sistem güvenliği politikaları, güvenli bir ağda olması gereken unsurları tanımlayan ve kurumların bilgi güvenliğinin sağlanması için ilgili yönergeleri içeren yazılı metinlerdir (Can ve Akbaş, 2014). Ağ ve sistem güvenliğinin sağlanması ve yönetimi için gereken kuralları tanımlar.

Çizelge 2.1. (devam) Hazırlanabilecek destekleyici politikalar ve açıklamaları

Geliştirme ve Destek Süreçleri Politikası	Yazılım geliştirme, temin, destek ve test süreçlerinin yönetimi için uyulması gereken kuralları tanımlayan politikadır. Güvenli yazılım geliştirme, sistem kabul testleri, sistem değişiklikleri, yazılım paketlerindeki kısıtlamalar, sistem güvenlik testleri gibi hususlara ilişkin kuralları kapsamaktadır.
Zararlı Yazılımlardan Korunma Politikası	Bilgisayar virüsleri, solucanlar, casus yazılımlar gibi kötü niyetli yazılımlardan korunmak için kuralları tanımlayan politikadır.
Olay Kaydetme ve İzleme Politikası	Kullanıcı hareketleri, hatalar, kural dışılıklar ve bilgi güvenliği olaylarını kaydetmek, saklamak ve düzenli olarak izlemeye yönelik kuralları tanımlayan politikadır.
Teçhizat Güvenliği Politikası	Üzerinde bilgi barındıran, bilgi işlemeye yarayan veya aracılık eden cihaz ve donanımın; fiziksel ve çevresel tehditlere karşı korunmasına yönelik kuralları tanımlayan politikadır. Teçhizatın güvenliğinin sağlanmasına, elden çıkarılmasına, yeniden kullanımına ilişkin hususları içermektedir.
Değişiklik ve Kapasite Yönetimi Politikası	Bilgi sistemlerinin güvenli işletimi için kuralları tanımlayan politikadır. Bilgi sistemleri altyapı kaynaklarının izlenmesi, kapasite planlamalarının yapılması, değişiklik süreçlerinin tasarlanması ve yönetilmesine ilişkin hususlar ele alınmaktadır.
Bilgi Sistemleri Edinim, Geliştirme ve Bakım Politikası	Yeni temin edilecek bilgi sistemleri için güvenlik gereksinimlerini veya var olan sistemlerin iyileştirilmelerine yönelik kuralları tanımlayan politikadır.
Varlık İmha Politikası	Bilgi varlıklarının imhasına ilişkin kuralları tanımlayan politikadır. Kullanım ömrünü dolduran, bundan sonra kullanılmayacağı bilinen bilgi teknolojileri varlıklarının imhası sırasında dikkat edilecek unsurlar bu politika içerisinde yer alır (TÜBİTAK BİLGEM YTE, 2021).
Bilgi Transfer Politikası	Bilgi transferi esnasında uyulması gereken güvenlik kurallarını tanımlayan politikadır. Bilgi sınıflandırmasına uygun olarak bilginin hangi yollarla transfer edilebileceğine dair hususları içermektedir.
İnsan Kaynakları Yönetimi Politikası	Kurumun mevcut çalışanlarına yönelik bilgi güvenliği sorumluluklarını tanımlayan politikadır. İstihdam öncesi, çalışma esnası ve sonrasında uyulması gereken kuralları içermektedir.

3. YÖNTEM

3.1. Araştırmanın Modeli

Araştırmada yöntem olarak, olgu ve olayları nesnelleştirerek gözlemlenebilir, ölçülebilir ve sayısal olarak ifade edilebilir bir şekilde ortaya koymaya yarayan (Gurbetoğlu, 2018) nicel araştırma yöntemi kullanılmıştır. Araştırmada kamu kurumlarının bilgi güvenliği politikalarının kurumsal bilgi güvenliğinin sağlanması açısından etkinliğine ilişkin mevcut durumunun ortaya konulması amaçlandığından, hali hazırda var olan bir durumun var olduğu haliyle betimlenmesinde kullanılan (Karasar, 1999) betimsel tarama modeli kullanılmıştır. Bu kapsamda mevcut durumun analiz edilebilmesi için anket çalışması yapılmıştır. Araştırmaya katılan katılımcılara araştırmacı tarafından hazırlanan anketin uygulanması ile nicel veriler elde edilmiştir.

3.2. Araştırmanın Evreni ve Örneklemi

"Elektronik Kamu Bilgi Yönetim Sistemi"nde (KAYSİS) yer alan bakanlıklar ve bu bakanlıklar ile bağlı/ilgili/ilişkili kurumlar araştırma evrenini oluşturmaktadır. Adalet Bakanlığı, Aile ve Sosyal Hizmetler Bakanlığı, Çalışma ve Sosyal Güvenlik Bakanlığı, Çevre, Şehircilik ve İklim Değişikliği Bakanlığı, Dışişleri Bakanlığı, Enerji ve Tabii Kaynaklar Bakanlığı, Gençlik ve Spor Bakanlığı, Hazine ve Maliye Bakanlığı, İçişleri Bakanlığı, Kültür ve Turizm Bakanlığı, Milli Eğitim Bakanlığı, Milli Savunma Bakanlığı, Sağlık Bakanlığı, Sanayi ve Teknoloji Bakanlığı, Tarım ve Orman Bakanlığı, Ticaret Bakanlığı ve Ulaştırma ve Altyapı Bakanlığı ve bu bakanlıklar ile bağlı/ilgili/ilişkili kurumlar araştırma evrenini oluşturan kurumlardır. Araştırma evreninin geniş olması sebebiyle örneklem alma yoluna gidilmiştir.

Örneklem, evrene genelleme yapmaya olanak verecek biçimde evrenden belli sayıda bireyin seçilmesiyle oluşan katılımcı grubudur (İftar, 1999). Araştırmada olasılıklı örneklem yöntemlerinden biri olan küme örnekleme yöntemi kullanılmıştır. Küme örnekleme yönteminde, öncelikle evreni oluşturan birimler değil bu birimlerin bağlı bulunduğu kümeler ele alınır (Ankara Üniversitesi, 2012). Küme örnekleme tekniği, evrene giren bütün bireylerin listelenemediği ancak evrenin kendiliğinden alt gruplara ayrılmış olduğu ve bu alt gruplara giren bireylerin listelenebildiği durumlarda son derece kullanışlıdır (Earl, 2004).

Küme örnekleme yöntemiyle seçilen kurumlar, kritik altyapı sektörlerini düzenleyen ve bu kapsamda olmayan kurumlar olacak şekilde gruplara ayrılmıştır. Evren hacmi çok büyük ve birimler geniş bir coğrafi alana yayılmış olduğunda örneklemin evrendeki birimlerden rassal seçim yöntemi yaparak değil de, bu birimlerden oluşturulan gruplardan rassal seçim yapmak suretiyle oluşturulması daha etkili olabilir (Özmen, 1999). Küme örneklemesinde 4 olası durum vardır (Kapanoğlu, 2016).

Bunlar;

- Pratikte uygulaması zor olsa da eşit sayıda eleman içeren kümeler oluşturarak, her bir kümeden eşit sayıda örnek eleman seçilebilir.
- Değişen sayıda eleman içeren kümeler oluşturularak, her bir kümeden eşit sayıda örnek eleman seçilebilir.
- Eşit sayıda eleman içeren kümeler oluşturularak, her bir kümeden değişen sayıda örnek eleman seçilebilir.
- Değişen sayıda eleman içeren kümeler oluşturularak, her bir kümeden değişen sayıda örnek eleman seçilebilir (Türkiye Odalar ve Borsalar Birliği [TOBB], 2013).

Bu araştırmada, değişen sayıda eleman içeren kümeler oluşturularak, her bir kümeden değişen sayıda örnek eleman seçilmiştir (Kapanoğlu, 2016). CB DDO Rehber'de (2020) kritik altyapı "işlediği bilgi/verinin gizliliği, bütünlüğü veya erişilebilirliği bozulduğunda can kaybına, büyük ölçekli ekonomik zarara, ulusal güvenlik açıklarına veya kamu düzeninin bozulmasına yol açabilecek bilişim sistemlerini barındıran altyapılardır." şeklinde tanımlanmıştır. Asgari BG Kriterleri'nde (TÜBİTAK BİLGEM SGE, 2013) kamu kurumlarını kritik bilgi sistemleri[2] barındıran kritik kamu kurumları ve barındırmayan kurumlar diğer kurumlar olmak üzere sınıflandırılmıştır. Sektörel SOME Kurulum ve Yönetim Rehberi'nde (SOME Rehberi) kritik kamu hizmetleri[3] ifade edilmektedir (UDHB, 2014).

[2] Bir bilgi sisteminin bozulması veya yetkisiz erişimle karıştırılması halinde;
a. Enerji, su, acil yardım hizmetleri, gıda tedariki ve benzeri hayati hizmetlerin durması sonucunda can kaybı oluşması veya bazı bölgelerin boşaltılması,
b. Para piyasalarının durması, ulaştırma sistemlerinden birinin durması veya diğer nedenlerle ulusal ekonominin ciddi düzeyde zarara uğraması,
c. Ulusal güvenliğin sekteye uğraması
söz konusu oluyorsa o bilgi sistemi kritiktir. (TÜBİTAK BİLGEM SGE, 2013)

[3] Kritik Kamu hizmetleri; vatandaşın gündelik hayatında sıklıkla etkileşimde bulunduğu nüfus, tapu, vergi, ticaret, sosyal güvenlik, sağlık (acil servis, tıbbı hizmetler, kan ve organ bankacılığı ve halk sağlığı), gıda,

Örneklem belirlenirken kritik altyapı sektörlerini düzenleyen ve bu kapsamda olmayan kurumlara Rehber'de ve SOME Rehberi'nde yer alan tanımlardan ve Asgari BG Kriterleri'nde yapılan sınıflandırmadan yola çıkılarak karar verilmiştir.

Söz konusu sınıflandırmaya göre araştırma evrenini oluşturan 17 kamu kurumundan 12'si kritik altyapı sektörlerini düzenleyen kamu kurumları, 5'i ise bu kapsamda olmayan kamu kurumları olacak şekilde gruplandırılmıştır. Bu doğrultuda; araştırma evrenini oluşturan kurumlardan kritik altyapı sektörlerini düzenleyen kamu kurumlarından 4 tane, bu kapsamda olmayan kamu kurumlarından 2 tane seçilerek oransal olarak eşit bir dağılım gösterecek şekilde örneklem belirlenmiştir.

Örneklem olarak seçilen toplam 6 kamu kurumunda, bilgi işlem/bilgi sistemleri birimi çalışanlarından oluşan veya bilgi teknolojileri/güvenliği projelerinde görev alan 121 katılımcı araştırmaya katılım sağlamıştır.

3.3. Çalışma Grubu

Araştırmaya katılan kamu kurumlarının bilgi işlem/bilgi sistemleri birimi çalışanlarından veya bilgi teknolojileri/güvenliği projelerinde görev alan çalışanlardan oluşan 121 katılımcı araştırmanın çalışma grubunu oluşturmaktadır.

3.4. Veri Toplama Aracı

Araştırmanın en önemli aşamalarından biri de veri ve bilgi toplama yöntem ve aracının seçilmesidir (Odabaşı, 1999). Araştırma verilerinin toplanması için anket tekniğinden yararlanılmıştır. Anket; bireylerin demografik özelliklerini, tercihlerini belirlemek için ya da bir konu, durum, olay hakkında bilgi toplamaya yönelik çeşitli soruların bir araya getirilmesiyle oluşturulan veri toplama aracıdır (Metin, 2014). Kamu kurumlarının bilgi güvenliği politikalarının kurumsal bilgi güvenliğinin sağlanması açısından etkinliğinin analiz edilebilmesi için 55 sorudan oluşan bir anket geliştirilmiştir. Literatür taraması yapılmış ve hali hazırda bilgi güvenliği politikası bulunan kurumların politikaları, CB DDO

güvenlik (polis, jandarma, sahil güvenlik), yollar ve köprüler, barajlar, maaş ve adli işlemlerin yapıldığı ve kayıtlarının bulunduğu kritik sistemlerden sunulan servislerdir (UDHB, 2014).

Rehber, Rehber'e ilişkin 2019 yılında yayınlanmış olan Genelge, ISO 27001 BGYS Standardı EK-A kontrol maddeleri ve TÜBİTAK BİLGEM YTE tarafından Ocak 2021'de yayınlanan BGYR incelenerek anket soruları hazırlanmıştır. Her politikada ortak olan ve kurumların yapısına göre değişmeyecek nitelikte olan hususlar belirlenerek sorular hazırlanmıştır. Anket üç bölümden oluşmaktadır. Anketin birinci bölümünde katılımcılardan demografik bilgiler istenmektedir. Demografik bilgiler; cinsiyet, yaş, eğitim düzeyi, görev yapılan kurumda çalışma süresi ve çalışma alanı bilgilerinden oluşmaktadır. Anketin ikinci bölümünde kişilerin görev yaptıkları kurumun yapısını anlamaya yönelik sorulardan oluşan kurumsal bilgiler yer almaktadır. Kurumsal bilgiler; kurumun hizmet verdiği sektör bilgisi ve kurumun iş süreçlerinde bilgi sistemleri kullanım yoğunluğu bilgisinden oluşmaktadır. Anketin üçüncü bölümünde ise "Bilgi Güvenliği Politikalarının Etkinliği" başlıklı "Kesinlikle Katılıyorum", "Katılıyorum", "Ne Katılıyorum Ne Katılmıyorum", "Katılmıyorum" ve "Kesinlikle Katılmıyorum" dereceli 5'li likert ölçeği kullanılarak hazırlanan sorular yer almaktadır. "Bilgi Güvenliği Politikalarının Etkinliği" soruları; 48 maddeden oluşmaktadır. Anket Google Formlar web uygulaması aracılığıyla çevrimiçi olarak oluşturulmuştur. "Bilgi Güvenliği Politikalarının Etkinliği" anketinin 17 alt ana başlığı vardır. Alt ana başlıklara ilişkin ankette yer alan soru sayısı Çizelge 3.1'de verilmektedir.

Çizelge 3.1. Anket alt ana başlıklarına ilişkin soru sayıları

Numara	Alt Ana Başlıklar	Anket Soru Sayısı
1	Bilgi Güvenliği Politika Dokümanı	4
2	Bilgi Güvenliği Organizasyonu ve Sorumluluklar	6
3	Farkındalık ve Eğitim	2
4	Varlık Yönetimi	2
5	Risk Yönetimi	2
6	Parola Güvenliği	4
7	E-posta Güvenliği	1
8	Ağ, Sistem ve Erişim Güvenliği	9
9	Uygulama Güvenliği	3
10	İşletim Güvenliği	3
11	İş Sürekliliği Yönetimi	1
12	Tedarikçi İlişkilerinde Bilgi Güvenliği	2
13	Fiziksel Güvenlik	2
14	Temiz Masa Temiz Ekran	1
15	Taşınabilir Cihaz ve Ortam Güvenliği	4
16	İnsan Kaynakları Güvenliği	1
17	Bilgi Güvenliği İhlal Olay Yönetimi	1
	TOPLAM	48

3.5. Uzman Görüşü Alma

Ankette yer alan maddeler alanında uzman 2 istatistikçi ve bilgi güvenliği, sistem yönetimi ve yazılım geliştirme alanlarında uzman 3 teknik kişiyle incelenmiştir. Yazım yanlışı ve dilbilgisi hataları giderilmiştir. Alan uzmanlarının görüşleri alınarak geçerlik ve kullanışlılık için gerekli görülen düzeltmeler yapılmıştır. Anket soruların açık ve anlaşılır olmasına dikkat edilmiştir. Katılımcıların sorular üzerinde farklı anlamlar çıkarabilmesinin önüne geçilebilmesi için anket sorularına itina gösterilmiştir.

3.6. Verilerin Toplanması

Anket Google Formlar web uygulaması aracılığıyla çevrimiçi olarak oluşturulmuştur. Anketin uygulanarak verilerin toplanması; Ağustos - Eylül 2021 tarihleri arasındaki 1 aylık sürede gerçekleştirilmiştir.

3.7. Verilerin Analizi

Geçerlik - güvenirlik

Verilerin analiz edilmesinden önce veri toplama aracı olarak kullanılan anketin güvenilir olup olmadığının tespit edilmesi için geçerlik güvenirlik testleri yapılmıştır. Güvenirlik, ele alınan ölçüm aracının benzer şartlarda benzer girdilerle yapılan değişik ölçümlerde benzer sonuçları vermesidir (İslamoğlu ve Alnıaçık, 2016). Likert tipi ölçümlerde ölçeğin iç tutarlılığını belirlemede Cronbach Alpha yöntemi kullanılır (Kılıç, 2019).

- $0,00 \leq \alpha \leq 0,40$ ise ölçek güvenilir değildir.
- $0,40 \leq \alpha \leq 0,60$ ise ölçek düşük güvenilirliktedir.
- $0,60 \leq \alpha \leq 0,80$ ise ölçek oldukça güvenilirdir.
- $0,80 \leq \alpha \leq 1,00$ ise ölçek yüksek derecede güvenilir bir ölçektir.

Araştırmada uygulanan anket için geçerlik güvenirlik analizi sonucu Çizelge 3.2'de verilmektedir.

Çizelge 3.2. Anket geçerlik - güvenirlik analizi

Güvenirlik Katsayısı	
Cronbach's Alpha	Madde Sayısı
,960	48

Cronbach Alpha (α) güvenirlik katsayısı anketin tümü için ,96 olarak hesaplanmıştır. Bu sebeple; anketin yüksek derecede güvenilir olduğunu söylemek mümkündür.

Normallik testi sonuçları

Anketten elde edilen verilerin dağılım normalliğinin belirlenmesi amacıyla Kolmogorov-Smirnov ve Shapiro-Wilk normallik testleri uygulanmıştır. Bunun yanı sıra basıklık (kurtosis) ve çarpıklık (skewness) katsayıları da hesaplanmıştır. Anketten elde edilen verilere uygulanan basıklık ve çarpıklık katsayılarının -2, +2 arasında olduğu görülmüştür. Bu sebeple verilerin normal dağılım gösterdiği varsayılmıştır (Mallery ve Darren, 2010). Verilere uygulanan Kolmogorov-Smirnov ve Shapiro-Wilk normallik testleri sonucunda ise p değeri 0,05 anlamlılık değerinin üzerinde olduğu için verilerin normal dağıldığı hipotezi kabul edilmiş olup araştırma verilerinin analiz edilmesinde normal dağılım gösteren veriler için uygulanan parametrik testler tercih edilmiştir.

Uygulanacak veri analiz testleri

Katılımcıların demografik özellikleri için frekans ve yüzde gibi tanımlayıcı istatistiksel analizler kullanılmıştır. Katılımcıların cinsiyetlerine göre ankete verilen cevapların farklılaşıp farklılaşmadığının belirlenmesi amacıyla iki grup arasında karşılaştırma yapılmasında kullanılan bağımsız gruplar t testi uygulanmıştır. Verilere uygulanan normallik testi sonucunda verilerin normal dağıldığı hipotezi kabul edilerek normal dağılan veriler için uygulanan parametrik testlerden üç ya da daha fazla grup karşılaştırması için katılımcıların yaş, eğitim düzeyi, görev aldıkları kurumda çalışma süreleri ve çalışma alanları, kurumlarının sahip olduğu verilerin kritiklik düzeyleri ve kurumlarının iş süreçlerinde bilgi sistemleri kullanım yoğunluğuna göre ankete verilen cevapların farklılaşıp farklılaşmadığının belirlenmesi amacıyla tek yönlü varyans analizi (ANOVA) tekniği uygulanmıştır. Kurumların sahip olduğu verilerin kritiklik düzeyleri ve iş süreçlerinde bilgi

sistemleri kullanım yoğunluğu bağımsız değişkenlerine göre ankete verilen cevapların p anlamlılık değeri <0,05 olduğu için istatistiksel açıdan anlamlı farklılıklar bulunmaktadır. Ancak araştırmanın temel amacının kurumların bilgi güvenliği politikalarının etkinliğinin incelenmesi olduğu için anketi dolduran katılımcıların kişisel görüş ve nitelikleri ile ilgili olmamasından dolayı beklenildiği üzere diğer bağımsız değişkenler için ankete verilen cevapların p anlamlılık değeri 0,05'in üzerinde olduğundan anlamlı bir farklılık görülmemiştir. Bu nedenle Kurumların sahip olduğu verilerin kritiklik düzeyleri ve iş süreçlerinde bilgi sistemleri kullanım yoğunluğu bağımsız değişkenleri için uygulanan ANOVA tekniği sonrasında anlamlı farklılıklar tespit edildikten sonra varyansların homojenliği testi uygulanmıştır. Varyansların homojenliği testi sonrası varyansların eşit olduğu kabul edilerek ve hangi gruplar arasında anlamlı farklılıklar olduğunun anlaşılması amacıyla çoklu karşılaştırma post hoc testlerden Tukey HSD testi uygulanmıştır. Elde edilen verilerin analizinde SPSS 28.0 istatistik paket programı kullanılmıştır.

4. ARAŞTIRMA BULGULARI

Bu bölümde, ankete katılım sağlayan katılımcılara ilişkin demografik özelliklere ve araştırma amacına yönelik belirlenen araştırma sorularına ait toplanan verilerle ilgili bulgulara ve değerlendirmelere yer verilmiştir.

4.1. Demografik Özellikler

Çalışma grubuna ait cinsiyet, yaş, eğitim düzeyi, görev yapılan kurumda çalışma süresi ve çalışma alanı bağımsız değişkenlerine ait frekans ve yüzde değerleri bu bölümde çizelgeler halinde verilmiştir.

Çizelge 4.1. Cinsiyete göre dağılım

Bağımsız Değişken		N	Yüzde (%)
Cinsiyet	Kadın	42	34,70
	Erkek	79	65,30
	Toplam	121	100,00

Çizelge 4.1 incelendiğinde katılımcıların %34,70'ini (N=42) kadınların ve %65,30'unu (N=79) erkeklerin oluşturduğu görülmektedir.

Çizelge 4.2. Yaşa göre dağılım

Bağımsız Değişken		N	Yüzde (%)
Yaş	21-30	31	25,60
	31-40	54	44,60
	41-50	27	22,30
	50 yaş üzeri	9	7,40
	Toplam	121	100,00

Çizelge 4.2'de araştırmaya katılan katılımcıların yaş gruplarına bakıldığında, %25,60'ı (N=31) 21-30 yaş grubunda, %44,60'ı (N=54) 31-40 yaş grubunda, %22,30'u (N=27) 41-50 yaş grubunda ve %7,40'ı (N=9) 50 yaş grubundadır.

Çizelge 4.3. Eğitim düzeyine göre dağılım

Bağımsız Değişken		N	Yüzde (%)
Eğitim Düzeyi	Lise ve altı	1	0,80
	Ön Lisans	3	2,50
	Lisans	63	52,10
	Yüksek Lisans	42	34,70
	Doktora	12	9,90
	Toplam	121	100,00

Çizelge 4.3'te görüleceği üzere, katılımcıların %0,80'i (N=1) lise ve altı öğrenim düzeyine sahip, %2,50'si (N=3) ön lisans, %52,10'ı (N=63) lisans, %34,70'i (N=42) yüksek lisans ve %9,90'ı (N=12) doktora öğrenim düzeyine sahiptir.

Çizelge 4.4. Çalışma süresine göre dağılım

Bağımsız Değişken		N	Yüzde (%)
Çalışma Süresi	1 yıl ve daha az	8	6,60
	2-5 yıl	26	21,50
	6-10 yıl	49	40,50
	11-14 yıl	21	17,40
	15 yıl ve üzeri	17	14,00
	Toplam	121	100,00

Çizelge 4.4'te katılımcıların görev yaptıkları kurumdaki çalışma süresine bakıldığında, %6,60'ı (N=8) 1 yıl ve daha az, %21,50 (N=26) 2-5 yıl, %40,50'si (N=49) 6-10 yıl, %17,40'ı (N=21) 11-14 yıl ve %14'ü (N=17) 15 yıl ve üzeri çalışma süresine sahiptir.

Çizelge 4.5. Çalışma alanına göre dağılım

Bağımsız Değişken		N	Yüzde (%)
Çalışma Alanı	Yazılım Geliştirme	28	23,10
	Yazılım Kalite ve Test	2	1,70
	Mobil Uygulama Geliştirme	4	3,30
	Ağ ve Sistem Yönetimi	14	11,60
	Bilgi Güvenliği/Siber Güvenlik	33	27,30
	Veri Tabanı Yönetimi	7	5,80
	Bilgi İşlem Teknik Destek	6	5,00
	Bilgi Teknolojileri Denetimi	3	2,50
	Bilgi Teknolojileri Proje Yönetimi	5	4,10
	Diğer	19	15,70
	Toplam	121	100,00

Çizelge 4.5'te görüleceği üzere, katılımcıların %23,10'u (N=28) yazılım geliştirme, %1,70'i (N=2) yazılım kalite ve test, %3,30'u (N=4) mobil uygulama geliştirme, %11,60'ı (N=14) ağ ve sistem yönetimi, %27,30'u (N=33) bilgi güvenliği/siber güvenlik, %5,80'i (N=7) veri tabanı yönetimi, %5,00'ı (N=6) bilgi işlem teknik destek, %2,50'si (N=3) bilgi teknolojileri denetimi, %4,10'u (N=5) bilgi teknolojileri proje yönetimi alanlarında çalışmaktadır. %15,70'i ise (N=19) çalışma alanını diğer olarak işaretlemiştir.

4.2. Kurumsal Yapı Özellikleri

Katılımcıların görev aldıkları kurumların kurumsal yapılarını anlamaya yönelik olarak sorulan sorulara ilişkin elde edilen verilerin frekans ve yüzde değerleri bu bölümde çizelgeler halinde verilmektedir.

Çizelge 4.6. Kurumun sahip olduğu verilerin kritiklik düzeyine göre dağılım

Bağımsız Değişken		N	Yüzde (%)
Kurumun Sahip Olduğu Verilerin Kritiklik Düzeyi	Çok Düşük	10	8,30
	Düşük	17	14,00
	Orta	36	29,80
	Yüksek	33	27,30
	Çok Yüksek	25	20,70
	Toplam	121	100,00

Çizelge 4.6'da araştırmaya katılan katılımcıların görev aldıkları kurumun sahip olduğu verilerin kritiklik düzeylerine bakıldığında %8,30'unun (N=10) çok düşük, %14,00'ının (N=17) düşük, %29,80'inin (N=36) orta, %27,30'unun (N=33) yüksek ve %20,70'inin (N=25) çok yüksek olduğu görülmektedir.

Çizelge 4.7. İş süreçlerinde bilgi sistemleri kullanım yoğunluğuna göre dağılım

Bağımsız Değişken		N	Yüzde (%)
Kurumun İş Süreçlerinde Bilgi Sistemlerinin Kullanılma Yoğunluğu	Çok Düşük	8	6,60
	Düşük	15	12,40
	Orta	22	18,20
	Yüksek	44	36,40
	Çok Yüksek	32	26,40
	Toplam	121	100,00

Çizelge 4.7'de katılımcıların görev aldıkları kurumun iş süreçlerinde bilgi sistemleri kullanım yoğunluğuna bakıldığında %6,60'ının (N=8) çok düşük, %12,40'ının (N=15) düşük, %18,20'sinin (N=22) orta, %36,40'ının (N=44) yüksek ve %26,40'ının (N=32) çok yüksek olduğu görülmektedir.

4.3. Anket Soruları Ortalama ve Standart Sapma Değerleri

Anket sorularına katılımcılar tarafından verilen cevapların ortalama ve standart sapma değerleri Çizelge 4.8'de verilmiştir.

Çizelge 4.8. Anket soruları ortalama ve standart sapma değerleri

Alt Ana Başlık	Soru No	Anket Soruları	Ort	Ss
Bilgi Güvenliği Politika Dokümanı	1	Bilgi güvenliği politikası açık ve anlaşılır bir dilde yazılmıştır.	4,16	0,77
	2	Bilgi güvenliği politikası bilgi güvenliği gereksinimlerine uygun şekilde hareket etmem konusunda yeterince yol göstericidir.	3,95	0,96
	3	Bilgi güvenliği politikası tüm çalışanların erişebileceği bir alanda tutulmaktadır.	4,23	0,76
	4	Bilgi güvenliği politikası kapsamında diğer dokümanlar (politika, prosedür, form, iş süreci ve talimat) oluşturulmuştur.	4,20	0,69
Bilgi Güvenliği Organizasyonu ve Sorumluluklar	5	Bilgi güvenliğinin sağlanması konusunda koordinasyonu sağlayacak bir bilgi güvenliği koordinasyon kurulu/yönetimi vardır.	4,14	0,76
	6	Yönetim, bilgi sisteminin kurum amaçlarına uygun çalışmasını ve işlevlerini doğru bir şekilde yerine getirmesini sağlayacak tedbirleri almaktadır.	3,92	0,81
	7	Yürütülen çalışmalarda görevler ayrılığı ilkesine uygun davranılmaktadır.	3,31	1,26
	8	İş süreçlerinde görevler ayrılığı ilkesinin uygulanabilmesi için yeterli sayıda ve nitelikte personel bulunmaktadır.	3,03	1,24
	9	Bilgi güvenliğinin sağlanması açısından en az yetki ve bilmesi gereken prensibine uygun hareket edilmektedir.	3,71	1,11
	10	Bilgi güvenliği çalışmaları iyi bir şekilde yönetilmektedir.	3,67	0,96
Farkındalık ve Eğitim	11	Gerçekleştirilen bilgi güvenliği farkındalık çalışmaları yeterli ve amacına uygundur.	3,52	1,03
	12	Yönetim, bilgi teknolojileri alanında çalışan ve bilgi güvenliği organizasyonunda yer alan personelin güncel bilgi güvenliği konularından haberdar olması adına personel gelişimini destekleyici tutum ve davranışlar ortaya koymaktadır.	3,08	1,17
Varlık Yönetimi	13	Sahip olunan bilgi varlıklarına ilişkin envanter tutulmaktadır ve güncelliği sağlanmaktadır.	3,33	1,19

Çizelge 4.8. (devam) Anket soruları ortalama ve standart sapma değerleri

Varlık Yönetimi	14	Bilgi varlıklarının gizlilik değerlerine ilişkin bilgi sınıflandırması (gizli, çok gizli vb.) yapılmaktadır.	3,92	0,99
Risk Yönetimi	15	Sahip olunan bilgi varlıklarına ilişkin etkin bir risk değerlendirme çalışması yapılmaktadır.	3,19	1,17
	16	Risklere karşı tanımlanan düzeltici ve iyileştirici faaliyetler yeterli seviyededir.	3,58	0,94
Parola Güvenliği	17	Sistem, parolamı belirli uzunluk ve karmaşıklıkta oluşturmak için beni zorlamaktadır.	4,28	0,93
	18	Sistem, parolamı belirli aralıklarla değiştirmem için beni zorlamaktadır.	4,14	1,09
	19	Sistem, önceden kullandığım parolaları tekrar kullanmama izin vermemektedir.	4,29	0,96
	20	Sahip olduğum kullanıcı adı ve parola gibi bilgilerin gizliliği tarafımca yeterli bir şekilde sağlanmaktadır.	4,40	0,74
E-posta Güvenliği	21	E-posta güvenliğine ilişkin çözümler (spam koruması, zararlı bağlantılara erişimin engellenmesi vb.) uygulanmaktadır.	4,31	0,70
Ağ, Sistem ve Erişim Güvenliği	22	Kurum ağına bağlı sahip olduğum cihazlarda antivirüs programı çalışmaktadır.	4,39	0,86
	23	Yetkisiz erişimler de dâhil olmak üzere iç ağı, dış tehditlerden korumak için güvenlik önlemleri (güvenlik duvarı vb.) alınmaktadır.	4,33	0,72
	24	Kurumsal uygulamalara erişim sağlarken kimlik doğrulama mekanizması kullanılmaktadır.	4,35	0,87
	25	Kritik sistemlere erişimde çoklu kimlik/çok faktörlü doğrulama mekanizmaları (MFA, 2FA) kullanılmaktadır.	3,26	1,33
	26	Son kullanıcı aktiviteleri (log, denetim izi) güvenlik zafiyetleri ve bilgi sızdırmalarına karşı kayıt altına alınmaktadır.	4,17	0,82
	27	Kurum ağından güvenilir olmayan sitelere erişim kısıtlanmaktadır.	4,32	0,82
	28	Kurum ağına uzaktan erişim yalnızca güvenli uzaktan bağlantı sağlayan sistemler (VPN vb.) üzerinden gerçekleştirilmektedir.	3,72	1,32
	29	Kurum ağının saldırılara karşı korunabilmesi için gerekli güvenlik çözümleri (IPS, IDS, DDoS, WAF vb.) kullanılmaktadır.	4,28	0,72
	30	Düzenli olarak sızma testi ve güvenlik denetimleri gerçekleştirilmektedir.	3,34	1,24
Uygulama Güvenliği	31	Bağlantı yaptığım sistemde uzun süre aktif olmadığım durumda bağlantımın sona erdirilmesi için oturum zaman aşımı süresi çözümü uygulanmaktadır.	4,25	0,77
	32	Kurum bünyesinde geliştirilen uygulamalarda güvenli yazılım geliştirme yaşam döngüsü süreçleri ve modellerinden faydalanılmaktadır.	3,69	0,92
	33	Uygulama güvenliği için önlemler (sql injection, xss saldırılarının önlenmesine yönelik çalışmalar, insan robot davranışlarını birbirinden ayırt etmeye yarayan captcha çözümleri vb.) alınmaktadır.	3,95	0,86
İşletim Güvenliği	34	Bilgi güvenliğini etkileyen kurum iş süreçleri, bilgi işleme olanakları ve sistemlerdeki değişikliklere ilişkin planlama ve test çalışmaları yapılmaktadır.	3,22	1,17

Çizelge 4.8. (devam) Anket soruları ortalama ve standart sapma değerleri

İşletim Güvenliği	35	Yürütülen çalışmalarda geliştirme, test ve üretim ortamları mantıksal olarak birbirinden ayrılmıştır.	3,88	1,00
	36	Yürütülen çalışmalarda bilgi güvenliği gereksinimleri için etkin bir test süreci işletilmektedir.	3,48	1,13
İş Sürekliliği Yönetimi	37	Olası felaket durumlarında veya iş akışını engelleyecek, aksatacak her türlü senaryonun gerçekleşmesi halinde, bilgi güvenliği sürekliliğinin sağlanması için gerekli önlemler alınmaktadır.	3,81	1,01
Tedarikçi İlişkilerinde Bilgi Güvenliği	38	Tedarikçiler ve üçüncü taraf çalışanları ile gizlilik anlaşmaları yapılmaktadır.	4,18	0,74
	39	Tedarikçiler tarafından sağlanan hizmetlerde bilgi güvenliği riskleri oluşturabilecek durumlara karşı dikkatli davranılmaktadır.	4,04	0,88
Fiziksel Güvenlik	40	Kurum binasında fiziksel güvenlik önlemleri alınmaktadır.	4,24	0,79
	41	Belirli alanlara giriş ve çıkışlarda elektronik kapı, turnike, görüntü/ses kayıtları gibi fiziksel güvenlik önlemleri uygulanmaktadır.	4,34	0,73
Temiz Masa Temiz Ekran	42	Bilgisayar monitörlerinde, çalışma masası üstlerinde, bilgisayar kasalarında güvenlik ihlaline neden olacak nitelikte parola, gizli bilgi, belge vb. bulundurulmaması konusunda özen gösterilmektedir.	4,02	0,98
Taşınabilir Cihaz ve Ortam Güvenliği	43	Kritik bilgi barındıran ve yok edilmesi gereken ortamlar (belge, disk vs.) için imha kuralları işletilmektedir.	3,76	1,09
	44	İş ihtiyaçları için taşınabilir bellek kullanılması gerektiği durumlarda güvenlik tedbirleri (kurum tarafından yetkilendirilmiş ve kurum envanterine kaydedilmiş, parola ile erişim sağlanan taşınabilir bellek vb.) uygulanmaktadır.	3,59	1,33
	45	Mobil cihazlar üzerine yazılım kurulumuna yönelik kısıtlamalar uygulanmaktadır.	3,79	1,12
	46	Sahip olduğum kişisel cihazım ile kurum ağına bağlanmam gerektiği durumda gerekli güvenlik tedbirlerini uygulamaktadır.	4,14	0,89
İnsan Kaynakları Güvenliği	47	Bilgi varlıklarının amacına uygun kullanılmadığı durumlarda yaşanması muhtemel bilgi güvenliği ihlal olaylarından dolayı devreye girebilecek bir disiplin süreci oluşturulmuştur.	3,94	0,90
Bilgi Güvenliği İhlal Olay Yönetimi	48	Bilgi güvenliği ihlal olaylarına zamanında ve uygun karşılık verilebilmektedir.	3,89	0,82

4.4. Katılımcı Bilgileri Analiz Sonuçları

Katılımcıların cinsiyetlerine göre ankete verilen cevapların farklılaşıp farklılaşmadığının belirlenmesi amacıyla bağımsız gruplar t testi uygulanmıştır. Ankete verilen cevapların katılımcıların yaş, eğitim düzeyi, görev aldıkları kurumda çalışma süreleri ve çalışma alanlarının; bağlı oldukları kurumların sahip olduğu verilerin kritiklik düzeyleri ve iş

süreçlerinde bilgi sistemleri kullanım yoğunluğuna göre farklılaşıp farklılaşmadığının belirlenmesi amacıyla ANOVA tekniğinden yararlanılmıştır. Ancak araştırmanın temel amacının kurumların bilgi güvenliği politikalarının etkinliğinin incelenmesi olduğu için anketi dolduran katılımcıların kişisel görüş ve nitelikleri ile ilgili olmamasından dolayı beklenildiği üzere bu değişkenlere ilişkin elde edilen sonuçlarda anlamlı bir farklılık görülmediği tespit edilmiştir.

Cinsiyet için bağımsız gruplar t-testi sonuçları

Çizelge 4.9'da katılımcıların anketin tümü için elde ettikleri ortalama puanlar, puanlar arasındaki karşılaştırmayı gösteren t değeri ve p anlamlılık değeri sunulmuştur. Çizelgede de belirtildiği üzere cinsiyet değişkenine ilişkin anketin tümü için elde edilen sonuçlara bakıldığında p anlamlılık değeri 0,05'in üzerinde olduğundan anlamlı bir farklılık görülmediği tespit edilmiştir.

Çizelge 4.9. Cinsiyet için bağımsız gruplar t-testi sonuçları

Cinsiyet	N	Ort.	Ss	Sd	t	p
Kadın	42	3,79	0,59	119	-1,473	0,926
Erkek	79	3,95	0,56			

Yaş için ANOVA sonuçları

Çizelge 4.10'da katılımcıların anketin tümü için elde ettikleri ortalama puanlar, ortalama puanlar arasındaki farkın anlamlı olup olmadığının belirlenmesi için yapılan ANOVA sonuçları ve p anlamlılık değeri sunulmuştur. Çizelgede de belirtildiği üzere yaş değişkenine ilişkin anketin tümü için elde edilen sonuçlara bakıldığında p anlamlılık değeri 0,05'in üzerinde olduğundan anlamlı bir farklılık görülmediği tespit edilmiştir.

Çizelge 4.10. Yaş için ANOVA sonuçları

	Grup	Frekans (f)	Ortalama	Standart Sapma
Yaş	21-30	31	3,80	0,54
	31-40	54	4,01	0,55
	41-50	27	3,78	0,67
	50 yaş üzeri	9	3,84	0,43
	Toplam	121	3,89	0,57

	Kareler Toplamı	Serbestlik Derecesi	Kareler Ortalaması	F	p
Gruplar Arası	1,333	3	0,444	1,346	0,263
Grup İçi	38,623	117	0,333		
Toplam	39,956	120			

Eğitim için ANOVA sonuçları

Çizelge 4.11'de katılımcıların anketin tümü için elde ettikleri ortalama puanlar, ortalama puanlar arasındaki farkın anlamlı olup olmadığının belirlenmesi için yapılan ANOVA sonuçları ve p anlamlılık değeri sunulmuştur. Çizelgede de belirtildiği üzere eğitim düzeyi değişkenine ilişkin anketin tümü için elde edilen sonuçlara bakıldığında p anlamlılık değeri 0,05'in üzerinde olduğundan anlamlı bir farklılık görülmediği tespit edilmiştir.

Çizelge 4.11. Eğitim için ANOVA sonuçları

	Grup	Frekans (f)	Ortalama	Standart Sapma
Eğitim Düzeyi	Lise ve altı	1	4,00	-
	Ön Lisans	3	4,27	0,64
	Lisans	63	3,90	0,54
	Yüksek Lisans	42	3,86	0,61
	Doktora	12	3,81	0,61
	Toplam	121	3,89	0,57

	Kareler Toplamı	Serbestlik Derecesi	Kareler Ortalaması	F	p
Gruplar Arası	0,567	4	0,142	0,417	0,796
Grup İçi	39,389	116	0,340		
Toplam	39,956	120			

Çalışma süresi için ANOVA sonuçları

Çizelge 4.12'de katılımcıların anketin tümü için elde ettikleri ortalama puanlar, ortalama puanlar arasındaki farkın anlamlı olup olmadığının belirlenmesi için yapılan ANOVA sonuçları ve p anlamlılık değeri sunulmuştur. Çizelgede de belirtildiği üzere çalışma süresi

değişkenine ilişkin anketin tümü için elde edilen sonuçlara bakıldığında p anlamlılık değeri 0,05'in üzerinde olduğundan anlamlı bir farklılık görülmediği tespit edilmiştir.

Çizelge 4.12. Çalışma süresi için ANOVA sonuçları

	Grup	Frekans (f)	Ortalama	Standart Sapma
Çalışma Süresi	1 yıl ve daha az	8	3,94	0,71
	2-5 yıl	26	3,87	0,46
	6-10 yıl	49	3,89	0,49
	11-14 yıl	21	3,95	0,84
	15 yıl ve üzeri	17	3,85	0,54
	Toplam	121	3,89	0,57

	Kareler Toplamı	Serbestlik Derecesi	Kareler Ortalaması	F	p
Gruplar Arası	0,126	4	0,032	0,092	0,985
Grup İçi	39,830	116	0,343		
Toplam	39,956	120			

Çalışma alanı için ANOVA sonuçları

Çizelge 4.13'te katılımcıların anketin tümü için elde ettikleri ortalama puanlar, ortalama puanlar arasındaki farkın anlamlı olup olmadığının belirlenmesi için yapılan ANOVA sonuçları ve p anlamlılık değeri sunulmuştur. Çizelgede de belirtildiği üzere çalışma alanı değişkenine ilişkin anketin tümü için elde edilen sonuçlara bakıldığında p anlamlılık değeri 0,05'in üzerinde olduğundan anlamlı bir farklılık görülmediği tespit edilmiştir.

Çizelge 4.13. Çalışma alanı için ANOVA sonuçları

	Grup	Frekans (f)	Ortalama	Standart Sapma
Çalışma Alanı	Yazılım Geliştirme	28	3,88	0,53
	Yazılım Kalite ve Test	2	3,63	1,04
	Mobil Uygulama Geliştirme	4	4,20	0,61
	Ağ ve Sistem Yönetimi	14	4,01	0,64
	Bilgi Güvenliği/Siber Güvenlik	33	3,95	0,58
	Veri Tabanı Yönetimi	7	3,85	0,26
	Bilgi İşlem Teknik Destek	6	3,76	0,65
	Bilgi Teknolojileri Denetimi	3	3,88	0,39
	Bilgi Teknolojileri Proje Yönetimi	5	3,90	0,19
	Diğer	19	3,74	0,70
	Toplam	121	3,89	0,57

	Kareler Toplamı	Serbestlik Derecesi	Kareler Ortalaması	F	p
Gruplar Arası	1,363	9	0,151	0,435	0,913
Grup İçi	38,594	111	0,348		
Toplam	39,956	120			

4.5. Araştırma Sorularına İlişkin Bulgular

4.5.1. Birinci araştırma sorusuna ilişkin bulgular

Anket sonuçları değerlendirilirken; "Kesinlikle Katılıyorum" seçeneği 5, "Katılıyorum" seçeneği 4, "Ne Katılıyorum Ne Katılmıyorum" seçeneği 3, "Katılmıyorum" seçeneği 2 ve "Kesinlikle Katılmıyorum" seçeneği 1 olacak şekilde tüm seçenekler için katsayılar belirlenmiştir.

Çizelge 4.14. Bilgi güvenliği politikalarının etkinliğine ilişkin sonuçlar

Alt Ana Başlıklar	Anket Soru Sayısı	Katsayı Ortalaması	Yüzde Oranı
1. Bilgi Güvenliği Politika Dokümanı	4	4,13	82,70
2. Bilgi Güvenliği Organizasyonu ve Sorumluluklar	6	3,63	72,60
3. Farkındalık ve Eğitim	2	3,30	66,00
4. Varlık Yönetimi	2	3,62	72,50
5. Risk Yönetimi	2	3,38	67,70
6. Parola Güvenliği	4	4,27	85,55
7. E-posta Güvenliği	1	4,31	86,20
8. Ağ, Sistem ve Erişim Güvenliği	9	4,01	80,36
9. Uygulama Güvenliği	3	3,96	79,27
10. İşletim Güvenliği	3	3,52	70,53
11. İş Sürekliliği Yönetimi	1	3,81	76,20
12. Tedarikçi İlişkilerinde Bilgi Güvenliği	2	4,11	82,20
13. Fiziksel Güvenlik	2	4,29	85,80
14. Temiz Masa Temiz Ekran	1	4,02	80,40
15. Taşınabilir Cihaz ve Ortam Güvenliği	4	3,82	76,40
16. İnsan Kaynakları Güvenliği	1	3,94	78,80
17. Bilgi Güvenliği İhlal Olay Yönetimi	1	3,89	77,80
Toplam	48	3,89	77,80

Çizelge 4.14'te, anketin alt ana başlıkları, her ana başlığa ait anketteki soru sayısı, her alt ana başlıktaki sorular için katılımcılar tarafından verilen cevapların katsayı ortalamaları ve bu ortalamaların yüzde oranları verilmiştir. Örnek olarak çizelgeden; ağ, sistem ve erişim güvenliğine ilişkin ankette 9 soru sorulduğu, bu sorulara ilişkin katılımcılar tarafından verilen cevapların katsayılarının ortalamasının 4,01 olduğu ve bu değerin %80,36'ya karşılık geldiği çıkarılabilmektedir.

Çizelge 4.14 bütünüyle değerlendirildiğinde, anketteki tüm sorular için katsayı ortalamasının 3,89 olduğu görülmektedir. Buna bağlı olarak, seçilen örneklem kümesinde

yer alan kamu kurumlarının bilgi güvenliği politikalarının %77,80 oranında etkin olduğu söylenebilir. Ayrıca, en etkin olan güvenlik konularının 4,31 katsayısı ve %86,20 oranı ile e-posta güvenliği ve 4,29 katsayısı ve %85,80 oranı ile fiziksel güvenlik olduğu ve en az etkin olan güvenlik konularının 3,30 katsayısı ve %66,00 oranı ile farkındalık ve eğitim ve 3,38 katsayısı ve %67,70 oranı ile risk yönetimi olduğu görülmektedir.

4.5.2. İkinci araştırma sorusuna ilişkin bulgular

Katılımcılar tarafından ankette yer alan sorulara verilen cevapların katsayı ortalamalarının, kamu kurumlarının sahip olduğu verilerin kritiklik düzeylerine göre istatistiksel açıdan anlamlı düzeyde farklılık gösterip göstermediğinin belirlenmesi amacıyla ANOVA tekniğinden yararlanılmıştır.

Çizelge 4.15. Kurumun sahip olduğu verilerin kritiklik düzeyi ANOVA sonuçları

	Grup	Frekans (f)	Ortalama	Oran (%)	Standart Sapma
Kurumun Sahip Olduğu Verilerin Kritiklik Düzeyi	Çok Düşük	10	3,6104	72,20	0,48473
	Düşük	17	3,6728	73,40	0,43829
	Orta	36	3,8137	76,20	0,53944
	Yüksek	33	3,9122	78,20	0,61387
	Çok Yüksek	25	4,2575	85,00	0,55309
	Total	121	3,8957	77,80	0,57703

	Kareler Toplamı	Serbestlik Derecesi	Kareler Ortalaması	F	p
Gruplar Arası	5,182	4	1,296	4,322	0,003
Grup İçi	34,774	116	0,3		
Toplam	39,956	120			

Çizelge 4.15'te; kurumun sahip olduğu verilerin kritiklik düzeyleri grupları, her grup için ankete kaç katılımcının yer aldığını gösteren frekans değeri, katılımcılar tarafından verilen cevapların katsayı ortalamaları, standart sapma değerleri, kareler toplamı, serbestlik derecesi, kareler ortalaması, test istatistiği (F değeri) ve anlamlılık değeri (p) verilmiştir.

Çizelge 4.15'teki frekans değerlerine bakılacak olursa, ankete kurumun sahip olduğu verilerin kritiklik düzeyi çok düşük olan 10 katılımcı, düşük olan 17 katılımcı, orta olan 36 katılımcı, yüksek olan 33 katılımcı ve çok yüksek olan 25 katılımcının katılım sağladığı görülmektedir. Katılımcılar tarafından verilen cevapların katsayı ortalamaları değerlendirildiğinde, çok düşük olan grubun 3,6104, düşük olan grubun 3,6728, orta olan grubun 3,8137, yüksek olan grubun 3,9122 ve çok yüksek olan grubun 4,2575 ortalama

katsayı değerlerine sahip olduğu ve yüzde oranlarının sırasıyla %72,20, %73,40, %76,20, %78,20 ve %85,00 olduğu görülmektedir. Böylece kurumun sahip olduğu verilerin kritiklik düzeyi arttıkça katsayı ortalamaları değerlerinin de arttığı, dolayısıyla bilgi güvenliği politikalarının etkinliğinin arttığı söylenebilmektedir.

Çizelge 4.15'te görüldüğü üzere p anlamlılık değeri 0,003 olarak hesaplanmıştır. Bu durumda p<0,05 olduğu için gruplar arasında istatistiki açıdan anlamlı farklılıklar bulunduğu belirlenmiştir. Hangi gruplar arasında anlamlı farklılıklar bulunduğuna ilişkin bilgiler Çizelge 4.16'da verilmiştir.

Böylece "*H1a: Kamu kurumlarının sahip olduğu verilerin kritiklik düzeyi ile bilgi güvenliği politikalarının etkinliği arasında istatistiksel açıdan anlamlı düzeyde bir farklılık bulunmaktadır."* hipotezi kabul edilmiştir.

Çizelge 4.16. Kurumun sahip olduğu verilerin kritiklik düzeyi Tukey HSD sonuçları

Kurumun Sahip Olduğu Verilerin Kritiklik Düzeyi		Ortalama Fark	p
Çok Düşük	Düşük	-0,06238	0,999
	Orta	-0,20324	0,837
	Yüksek	-0,30183	0,547
	Çok Yüksek	-,64708*	0,017
Düşük	Çok Düşük	0,06238	0,999
	Orta	-0,14086	0,906
	Yüksek	-0,23945	0,587
	Çok Yüksek	-,58471*	0,008
Orta	Çok Düşük	0,20324	0,837
	Düşük	0,14086	0,906
	Yüksek	-0,09859	0,945
	Çok Yüksek	-,44384*	0,019
Yüksek	Çok Düşük	0,30183	0,547
	Düşük	0,23945	0,587
	Orta	0,09859	0,945
	Çok Yüksek	-0,34525	0,129
Çok Yüksek	Çok Düşük	,64708*	0,017
	Düşük	,58471*	0,008
	Orta	,44384*	0,019
	Yüksek	0,34525	0,129

Çizelge 4.16'ya bakılacak olursa, çok düşük ile çok yüksek grubu için p değeri 0,017 olduğu görülmekte ve p<0,05 olduğu için iki grup arasında anlamlı farklılık olduğu değerlendirilmektedir. Benzer şekilde, düşük ile çok yüksek grubu (p=0,008) ve orta ile çok yüksek grubu (p=0,019) arasında da p<0,05 şartı sağlandığı için anlamlı farklılık olduğu değerlendirilmektedir. Diğer grup eşleştirmeleri için p<0,05 şartı sağlanmadığı için anlamlı farklılık bulunmamaktadır. Örneğin yüksek ile çok yüksek grubu için p değeri 0,129 olduğu görülmekte, böylece iki grup arasında anlamlı farklılık olmadığı değerlendirilmektedir. Çizelge 4.16'da anlamlı farklılık olan gruplar * işareti ile ifade edilmiştir.

Çizelge 4.16'da anlamlı olarak farklılık bulunan grup eşleştirmeleri için ortalama fark değerlerine bakılacak olursa, çok düşük ile çok yüksek arasında ortalama fark değeri 0,64708, düşük ile çok yüksek arasında 0,58471 ve orta ile çok yüksek arasında 0,44384 olacak şekilde büyükten küçüğe sıralanmaktadır. Böylece çok düşük ile çok yüksek grubu arasındaki ortalama fark değeri diğerlerinden daha yüksek olduğu için farklılık düzeyinin diğerlerinden daha anlamlı olduğu değerlendirilmektedir. Benzer şekilde düşük ile çok yüksek grupları arasındaki farklılık düzeyi de orta ile çok yüksek grupları arasındaki farklılık düzeyinden daha anlamlı olduğu değerlendirilmektedir.

Çalışmanın temel amacı doğrultusunda belirlenen 17 alt ana başlık kapsamında oluşturulmuş olan sorulara yönelik elde edilen bulgulardan, kurumlarının sahip olduğu verilerin kritiklik düzeyleri bağımsız değişkenine göre anlamlı farklılık gösterenler; bu bölümde çizelgeler halinde alt ana başlığı ve alt ana başlığa ilişkin sorular ifade edilmek üzere belirtilmiştir. Söz konusu sorulara yönelik elde edilen verilerden, bağımsız değişkenin grupları arasında anlamlı farklılık gösterenler çizelgelerde * işareti ile ifade edilmiştir. Anlamlı farklılık gösteren sorulara ilişkin kurumların sahip olduğu verilerin kritiklik düzeyleri bağımsız değişkeninin grupları arasında kareler toplamı, serbestlik derecesi, kareler ortalaması, test istatistiği (F değeri) ve anlamlılık değeri (p) verilmiştir.

Çizelge 4.17'de "Bilgi Güvenliği Organizasyonu ve Sorumluluklar" alt ana başlığında yer alan "*Yürütülen çalışmalarda görevler ayrılığı ilkesine uygun davranılmaktadır."* ve "*İş süreçlerinde görevler ayrılığı ilkesinin uygulanabilmesi için yeterli sayıda ve nitelikte personel bulunmaktadır."* sorularına ilişkin p değerinin 0,000 olduğu görülmekte ve dolayısıyla p<0,05 olduğu için bağımsız değişkenin grupları arasında anlamlı farklılıklar olduğunu söylemek mümkündür. Anlamlı olarak farklılık bulunan grup eşleştirmeleri için

ortalama fark değerlerine bakılacak olursa örneğin "*Yürütülen çalışmalarda görevler ayrılığı ilkesine uygun davranılmaktadır."* sorusu için çok düşük grubunun sırasıyla çok yüksek grubu ile 3,00000, yüksek grubu ile 2,49697, orta grubu ile 2,24444 ve düşük grubu ile 1,03529 ortalama fark değerlerinin büyükten küçüğe doğru sıralandığı görülmektedir. Böylece çok düşük grup ile çok yüksek grup arasındaki ortalama fark değeri, diğer gruplar arası karşılaştırma sonuç değerlerinden daha yüksek olduğu için bu iki grup arasındaki farklılık düzeyinin diğerlerinden daha anlamlı olduğu değerlendirilmektedir. "*İş süreçlerinde görevler ayrılığı ilkesinin uygulanabilmesi için yeterli sayıda ve nitelikte personel bulunmaktadır."* sorusu için çok düşük grubunun sırasıyla çok yüksek grubu ile 2,68000, yüksek grubu ile 2,13333, orta grubu ile 1,88333 ve düşük grubu ile 0,97647 ortalama fark değerlerinin büyükten küçüğe doğru sıralandığı görülmektedir.

Çizelge 4.17. Bilgi güvenliği organizasyonu ve sorumluluklar için analiz sonuçları

Yürütülen çalışmalarda görevler ayrılığı ilkesine uygun davranılmaktadır.	Grup	Çok Düşük	Düşük	Orta	Yüksek	Çok Yüksek
	Çok Düşük	-	-1,03529*	-2,24444*	-2,49697*	-3,00000*
	Düşük	1,03529*	-	-1,20915*	-1,46168*	-1,96471*
	Orta	2,24444*	1,20915*	-	-0,25253	-,75556*
	Yüksek	2,49697*	1,46168*	0,25253	-	-0,50303
	Çok Yüksek	3,00000*	1,96471*	,75556*	0,50303	-

	Kareler Toplamı	Serbestlik Derecesi	Kareler Ortalaması	F	p
Gruplar Arası	89,549	4	22,387	25,835	0,000
Grup İçi	100,517	116	0,867		
Toplam	190,066	120			

İş süreçlerinde görevler ayrılığı ilkesinin uygulanabilmesi için yeterli sayıda ve nitelikte personel bulunmaktadır.	Grup	Çok Düşük	Düşük	Orta	Yüksek	Çok Yüksek
	Çok Düşük	-	-0,97647	-1,88333*	-2,13333*	-2,68000*
	Düşük	1,03529*	-	-1,20915*	-1,46168*	-1,96471*
	Orta	2,24444*	1,20915*	-	-0,25253	-,75556*
	Yüksek	2,49697*	1,46168*	0,25253	-	-0,50303
	Çok Yüksek	2,68000*	1,70353*	,79667*	0,54667	-

	Kareler Toplamı	Serbestlik Derecesi	Kareler Ortalaması	F	p
Gruplar Arası	67,074	4	16,768	16,654	0,000
Grup İçi	116,794	116	1,007		
Toplam	183,868	120			

Çizelge 4.18'de "Farkındalık ve Eğitim" alt ana başlığında yer alan "*Yönetim, bilgi teknolojileri alanında çalışan ve bilgi güvenliği organizasyonunda yer alan personelin güncel bilgi güvenliği konularından haberdar olması adına personel gelişimini destekleyici tutum ve davranışlar ortaya koymaktadır."* sorusuna ilişkin p değerinin 0,000 olduğu görülmekte ve dolayısıyla $p<0,05$ olduğu için bağımsız değişkenin grupları arasında anlamlı farklılık olduğunu söylemek mümkündür. Anlamlı olarak farklılık bulunan grup

eşleştirmeleri için ortalama fark değerlerine bakılacak olursa çok düşük grubunun sırasıyla çok yüksek grubu ile 2,52000, yüksek grubu ile 2,25455, orta grubu ile 2,02222 ve düşük grubu ile 1,03529 ortalama fark değerlerinin büyükten küçüğe doğru sıralandığı görülmektedir. Bu sebeple kurumların sahip olduğu verilerin kritiklik düzeyleri arttıkça söz konusu alt ana başlık altında yer alan soruya ilişkin etkinliğin arttığı değerlendirilmektedir.

Çizelge 4.18. Farkındalık ve eğitim başlığı için analiz sonuçları

Yönetim, bilgi teknolojileri alanında çalışan ve bilgi güvenliği organizasyonunda yer alan personelin güncel bilgi güvenliği konularından haberdar olması adına personel gelişimini destekleyici tutum ve davranışlar ortaya koymaktadır.	Grup	Çok Düşük	Düşük	Orta	Yüksek	Çok Yüksek
	Çok Düşük	-	-1,03529*	-2,02222*	-2,25455*	-2,52000*
	Düşük	1,03529*	-	-,98693*	-1,21925*	-1,48471*
	Orta	2,02222*	,98693*	-	-0,23232	-0,49778
	Yüksek	2,25455*	1,21925*	0,23232	-	-0,26545
	Çok Yüksek	2,52000*	1,48471*	0,49778	0,26545	-

	Kareler Toplamı	Serbestlik Derecesi	Kareler Ortalaması	F	p
Gruplar Arası	63,071	4	15,768	18,272	0,000
Grup İçi	100,103	116	0,863		
Toplam	163,174	120			

Çizelge 4.19'da "Varlık Yönetimi" alt ana başlığında yer alan "*Sahip olunan bilgi varlıklarına ilişkin envanter tutulmaktadır ve güncelliği sağlanmaktadır."* sorusuna ilişkin p değerinin 0,000 olduğu görülmekte ve dolayısıyla $p<0,05$ olduğu için bağımsız değişkenin grupları arasında anlamlı farklılık olduğunu söylemek mümkündür. Anlamlı olarak farklılık bulunan grup eşleştirmeleri için ortalama fark değerlerine bakılacak olursa çok düşük grubunun sırasıyla çok yüksek grubu ile 2,76000, yüksek grubu ile 2,64848, orta grubu ile 2,35556 ve düşük grubu ile 1,03529 ortalama fark değerlerinin büyükten küçüğe doğru sıralandığı görülmektedir. Bu sebeple kurumların sahip olduğu verilerin kritiklik düzeyleri arttıkça söz konusu alt ana başlık altında yer alan soruya ilişkin etkinliğin arttığı değerlendirilmektedir.

Çizelge 4.19. Varlık yönetimi başlığı için analiz sonuçları

Sahip olunan bilgi varlıklarına ilişkin envanter tutulmaktadır ve güncelliği sağlanmaktadır.	Grup	Çok Düşük	Düşük	Orta	Yüksek	Çok Yüksek
	Çok Düşük	-	-1,03529*	-2,35556*	-2,64848*	-2,76000*
	Düşük	1,03529*	-	-1,32026*	-1,61319*	-1,72471*
	Orta	2,35556*	1,32026*	-	-0,29293	-0,40444
	Yüksek	2,64848*	1,61319*	0,29293	-	-0,11152
	Çok Yüksek	2,76000*	1,72471*	0,40444	0,11152	-

	Kareler Toplamı	Serbestlik Derecesi	Kareler Ortalaması	F	p
Gruplar Arası	86,357	4	21,589	29,550	0,000
Grup İçi	84,750	116	0,731		
Toplam	171,107	120			

Çizelge 4.20'de "Risk Yönetimi" alt ana başlığında yer alan "*Sahip olunan bilgi varlıklarına ilişkin etkin bir risk değerlendirme çalışması yapılmaktadır."* sorusuna ilişkin p değerinin 0,000 olduğu görülmekte ve dolayısıyla $p<0,05$ olduğu için bağımsız değişkenin grupları arasında anlamlı farklılık olduğunu söylemek mümkündür. Anlamlı olarak farklılık bulunan grup eşleştirmeleri için ortalama fark değerlerine bakılacak olursa çok düşük grubunun sırasıyla çok yüksek grubu ile 2,68000, yüksek grubu ile 2,34545, orta grubu ile 2,35556 ve düşük grubu ile 0,74118 ortalama fark değerlerinin büyükten küçüğe doğru sıralandığı görülmektedir. Bu sebeple kurumların sahip olduğu verilerin kritiklik düzeyleri arttıkça söz konusu alt ana başlık altında yer alan soruya ilişkin etkinliğin arttığı değerlendirilmektedir.

Çizelge 4.20. Risk yönetimi başlığı için analiz sonuçları

Sahip olunan bilgi varlıklarına ilişkin etkin bir risk değerlendirme çalışması yapılmaktadır.	Grup	Çok Düşük	Düşük	Orta	Yüksek	Çok Yüksek
	Çok Düşük	-	-0,74118	-2,35556*	-2,34545*	-2,68000*
	Düşük	0,74118	-	-1,61438*	-1,60428*	-1,93882*
	Orta	2,35556*	1,61438*	-	0,01010	-0,32444
	Yüksek	2,34545*	1,60428*	-0,01010	-	-0,33455
	Çok Yüksek	2,68000*	1,93882*	0,32444	0,33455	-

	Kareler Toplamı	Serbestlik Derecesi	Kareler Ortalaması	F	p
Gruplar Arası	86,988	4	21,747	32,238	0,000
Grup İçi	78,252	116	0,675		
Toplam	165,240	120			

Çizelge 4.21'de "Ağ, Sistem ve Erişim Güvenliği" alt ana başlığında yer alan "*Kritik sistemlere erişimde çoklu kimlik/çok faktörlü doğrulama mekanizmaları (MFA, 2FA) kullanılmaktadır."* sorusuna ilişkin p değerinin 0,000 olduğu görülmekte ve dolayısıyla $p<0,05$ olduğu için bağımsız değişkenin grupları arasında anlamlı farklılık olduğunu söylemek mümkündür. Anlamlı olarak farklılık bulunan grup eşleştirmeleri için ortalama fark değerlerine bakılacak olursa çok düşük grubunun sırasıyla çok yüksek grubu ile

2,92000, yüksek grubu ile 2,55758, orta grubu ile 2,13333 ve düşük grubu ile 0,91765 ortalama fark değerlerinin büyükten küçüğe doğru sıralandığı görülmektedir. "*Son kullanıcı aktiviteleri (log, denetim izi) güvenlik zafiyetleri ve bilgi sızdırmalarına karşı kayıt altına alınmaktadır."* sorusuna ilişkin p değerinin 0,038 olduğu görülmekte ve dolayısıyla p<0,05 olduğu için bağımsız değişkenin grupları arasında anlamlı farklılık olduğunu söylemek mümkündür. Anlamlı olarak farklılık bulunan grup eşleştirmeleri için ortalama fark değerlerine bakılacak olursa yüksek ile çok yüksek grup arasında 0,63030 ortalama fark değerinin olduğu görülmektedir. "*Kurum ağına uzaktan erişim yalnızca güvenli uzaktan bağlantı sağlayan sistemler (VPN vb.) üzerinden gerçekleştirilmektedir."* ve *"Düzenli olarak sızma testi ve güvenlik denetimleri gerçekleştirilmektedir."* sorularına ilişkin p değerlerinin 0,000 olduğu görülmekte ve dolayısıyla p<0,05 olduğu için her iki soru için de bağımsız değişkenin grupları arasında anlamlı farklılık olduğunu söylemek mümkündür. *"Kurum ağına uzaktan erişim yalnızca güvenli uzaktan bağlantı sağlayan sistemler (VPN vb.) üzerinden gerçekleştirilmektedir."* sorusuna ilişkin anlamlı olarak farklılık bulunan grup eşleştirmeleri için ortalama fark değerlerine bakılacak olursa çok düşük grubunun sırasıyla çok yüksek grubu ile 3,40000, yüksek grubu ile 3,16364, orta grubu ile 2,77222 ve düşük grubu ile 0,97647ortalama fark değerlerinin büyükten küçüğe doğru sıralandığı görülmektedir. *"Düzenli olarak sızma testi ve güvenlik denetimleri gerçekleştirilmektedir."* sorusuna ilişkin anlamlı olarak farklılık bulunan grup eşleştirmeleri için ortalama fark değerlerine bakılacak olursa çok düşük grubunun sırasıyla çok yüksek grubu ile 3,02000, yüksek grubu ile 2,57879, orta grubu ile 2,06111 ve düşük grubu ile 0,75882 ortalama fark değerlerinin büyükten küçüğe doğru sıralandığı görülmektedir. Dolayısıyla kurumların sahip olduğu verilerin kritiklik düzeyleri arttıkça söz konusu alt ana başlık altında yer alan Çizelge 4.21'de verilen sorulara ilişkin etkinliğin arttığı değerlendirilmektedir.

Çizelge 4.21. Ağ, sistem ve erişim güvenliği başlığı için analiz sonuçları

Kritik sistemlere erişimde çoklu kimlik/çok faktörlü doğrulama mekanizmaları (MFA, 2FA) kullanılmaktadır.	Grup	Çok Düşük	Düşük	Orta	Yüksek	Çok Yüksek
	Çok Düşük	-	-0,91765	-2,13333*	-2,55758*	-2,92000*
	Düşük	0,91765	-	-1,21569*	-1,63993*	-2,00235*
	Orta	2,13333*	1,21569*	-	-0,42424	-,78667*
	Yüksek	2,55758*	1,63993*	0,42424	-	-0,36242
	Çok Yüksek	2,92000*	2,00235*	,78667*	0,36242	-

	Kareler Toplamı	Serbestlik Derecesi	Kareler Ortalaması	F	p
Gruplar Arası	91,472	4	22,868	22,094	0,000
Grup İçi	120,065	116	1,035		
Toplam	211,537	120			

Son kullanıcı aktiviteleri (log, denetim izi) güvenlik zafiyetleri ve bilgi sızdırmalarına karşı kayıt altına alınmaktadır.	Grup	Çok Düşük	Düşük	Orta	Yüksek	Çok Yüksek
	Çok Düşük	-	-0,03529	0,17222	0,23030	-0,40000
	Düşük	0,03529	-	0,20752	0,26560	-0,36471
	Orta	-0,17222	-0,20752	-	0,05808	-0,57222
	Yüksek	-0,23030	-0,26560	-0,05808	-	-,63030*
	Çok Yüksek	0,40000	0,36471	0,57222	,63030*	-

	Kareler Toplamı	Serbestlik Derecesi	Kareler Ortalaması	F	p
Gruplar Arası	6,755	4	1,689	2,626	0,038
Grup İçi	74,601	116	0,643		
Toplam	81,355	120			

Kurum ağına uzaktan erişim yalnızca güvenli uzaktan bağlantı sağlayan sistemler (VPN vb.) üzerinden gerçekleştirilmektedir.	Grup	Çok Düşük	Düşük	Orta	Yüksek	Çok Yüksek
	Çok Düşük	-	-,97647*	-2,77222*	-3,16364*	-3,40000*
	Düşük	,97647*	-	-1,79575*	-2,18717*	-2,42353*
	Orta	2,77222*	1,79575*	-	-0,39141	-,62778*
	Yüksek	3,16364*	2,18717*	0,39141	-	-0,23636
	Çok Yüksek	3,40000*	2,42353*	,62778*	0,23636	-

	Kareler Toplamı	Serbestlik Derecesi	Kareler Ortalaması	F	p
Gruplar Arası	139,321	4	34,830	58,829	0,000
Grup İçi	68,679	116	0,592		
Toplam	208,000	120			

Düzenli olarak sızma testi ve güvenlik denetimleri gerçekleştirilmektedir.	Grup	Çok Düşük	Düşük	Orta	Yüksek	Çok Yüksek
	Çok Düşük	-	-0,75882	-2,06111*	-2,57879*	-3,02000*
	Düşük	0,75882	-	-1,30229*	-1,81996*	-2,26118*
	Orta	2,06111*	1,30229*	-	-0,51768	-,95889*
	Yüksek	2,57879*	1,81996*	0,51768	-	-0,44121
	Çok Yüksek	3,02000*	2,26118*	,95889*	0,44121	-

	Kareler Toplamı	Serbestlik Derecesi	Kareler Ortalaması	F	p
Gruplar Arası	103,120	4	25,780	36,335	0,000
Grup İçi	82,302	116	0,709		
Toplam	185,421	120			

Çizelge 4.22'de "Uygulama Güvenliği" alt ana başlığında yer alan "*Kurum bünyesinde geliştirilen uygulamalarda güvenli yazılım geliştirme yaşam döngüsü süreçleri ve modellerinden faydalanılmaktadır."* sorusuna ilişkin p değerinin 0,016 olduğu görülmekte ve dolayısıyla $p<0,05$ olduğu için bağımsız değişkenin grupları arasında anlamlı farklılık

olduğunu söylemek mümkündür. Anlamlı olarak farklılık bulunan grup eşleştirmeleri için ortalama fark değerlerine bakılacak olursa orta grup ile çok yüksek grup arasında 0,79889 ortalama fark değerinin olduğu görülmektedir.

Çizelge 4.22. Uygulama güvenliği başlığı için analiz sonuçları

Kurum bünyesinde geliştirilen uygulamalarda güvenli yazılım geliştirme yaşam döngüsü süreçleri ve modellerinden faydalanılmaktadır.	Grup	Çok Düşük	Düşük	Orta	Yüksek	Çok Yüksek
	Çok Düşük	-	-0,02353	0,43889	0,19394	-0,36000
	Düşük	0,02353	-	0,46242	0,21747	-0,33647
	Orta	-0,43889	-0,46242	-	-0,24495	-,79889*
	Yüksek	-0,19394	-0,21747	0,24495	-	-0,55394
	Çok Yüksek	0,36000	0,33647	,79889*	0,55394	-

	Kareler Toplamı	Serbestlik Derecesi	Kareler Ortalaması	F	p
Gruplar Arası	10,071	4	2,518	3,188	0,016
Grup İçi	91,615	116	0,790		
Toplam	101,686	120			

Çizelge 4.23'te "İşletim Güvenliği" alt ana başlığında yer alan "*Bilgi güvenliğini etkileyen kurum iş süreçleri, bilgi işleme olanakları ve sistemlerdeki değişikliklere ilişkin planlama ve test çalışmaları yapılmaktadır."* sorusuna ilişkin p değerinin 0,000 olduğu görülmekte ve dolayısıyla $p<0,05$ olduğu için bağımsız değişkenin grupları arasında anlamlı farklılık olduğunu söylemek mümkündür. Anlamlı olarak farklılık bulunan grup eşleştirmeleri için ortalama fark değerlerine bakılacak olursa çok düşük grubunun sırasıyla çok yüksek grubu ile 2,92000, yüksek grubu ile 2,40606, orta grubu ile 2,16111 ve düşük grubu ile 0,85882 ortalama fark değerlerinin büyükten küçüğe doğru sıralandığı görülmektedir. "*Yürütülen çalışmalarda bilgi güvenliği gereksinimleri için etkin bir test süreci işletilmektedir."* sorusuna ilişkin p değerinin 0,015 olduğu görülmekte ve dolayısıyla $p<0,05$ olduğu için bağımsız değişkenin grupları arasında anlamlı farklılık olduğunu söylemek mümkündür. Anlamlı olarak farklılık bulunan grup eşleştirmeleri için ortalama fark değerlerine bakılacak olursa orta grup ile çok yüksek grup arasında 0,87667 ortalama fark değerinin olduğu görülmektedir.

Çizelge 4.23. İşletim güvenliği başlığı için analiz sonuçları

Bilgi güvenliğini etkileyen kurum iş süreçleri, bilgi işleme olanakları ve sistemlerdeki değişikliklere ilişkin planlama ve test çalışmaları yapılmaktadır.	Grup	Çok Düşük	Düşük	Orta	Yüksek	Çok Yüksek
	Çok Düşük	-	-0,85882	-2,16111*	-2,40606*	-2,92000*
	Düşük	0,85882	-	-1,30229*	-1,54724*	-2,06118*
	Orta	2,16111*	1,30229*	-	-0,24495	-,75889*
	Yüksek	2,40606*	1,54724*	0,24495	-	-0,51394
	Çok Yüksek	2,92000*	2,06118*	,75889*	0,51394	-

	Kareler Toplamı	Serbestlik Derecesi	Kareler Ortalaması	F	p
Gruplar Arası	89,610	4	22,402	34,481	0,000
Grup İçi	75,366	116	0,650		
Toplam	164,975	120			

Yürütülen çalışmalarda bilgi güvenliği gereksinimleri için etkin bir test süreci işletilmektedir.	Grup	Çok Düşük	Düşük	Orta	Yüksek	Çok Yüksek
	Çok Düşük	-	0,68824	1,01667	0,67576	0,14000
	Düşük	-0,68824	-	0,32843	-0,01248	-0,54824
	Orta	-1,01667	-0,32843	-	-0,34091	-,87667*
	Yüksek	-0,67576	0,01248	0,34091	-	-0,53576
	Çok Yüksek	-0,14000	0,54824	,87667*	0,53576	-

	Kareler Toplamı	Serbestlik Derecesi	Kareler Ortalaması	F	p
Gruplar Arası	15,443	4	3,861	3,227	0,015
Grup İçi	138,788	116	1,196		
Toplam	154,231	120			

Çizelge 4.24'te "Bilgi Güvenliği İhlal Olay Yönetimi" alt ana başlığında yer alan "*Bilgi güvenliği ihlal olaylarına zamanında ve uygun karşılık verilebilmektedir."* sorusuna ilişkin p değerinin 0,013 olduğu görülmekte ve dolayısıyla p<0,05 olduğu için bağımsız değişkenin grupları arasında anlamlı farklılık olduğunu söylemek mümkündür. Anlamlı olarak farklılık bulunan grup eşleştirmeleri için ortalama fark değerlerine bakılacak olursa orta grup ile çok yüksek grup arasında 0,65667 ortalama fark değerinin olduğu görülmektedir.

Çizelge 4.24. Bilgi güvenliği ihlal olay yönetimi başlığı için analiz sonuçları

Bilgi güvenliği ihlal olaylarına zamanında ve uygun karşılık verilebilmektedir.	Grup	Çok Düşük	Düşük	Orta	Yüksek	Çok Yüksek
	Çok Düşük	-	0,35882	0,71667	0,48182	0,06000
	Düşük	-0,35882	-	0,35784	0,12299	-0,29882
	Orta	-0,71667	-0,35784	-	-0,23485	-,65667*
	Yüksek	-0,48182	-0,12299	0,23485	-	-0,42182
	Çok Yüksek	-0,06000	0,29882	,65667*	0,42182	-

	Kareler Toplamı	Serbestlik Derecesi	Kareler Ortalaması	F	p
Gruplar Arası	8,343	4	2,086	3,303	0,013
Grup İçi	73,260	116	0,632		
Toplam	81,603	120			

4.5.3. Üçüncü araştırma sorusuna ilişkin bulgular

Katılımcılar tarafından ankette yer alan sorulara verilen cevapların katsayı ortalamalarının, kamu kurumlarının iş süreçlerinde bilgi sistemleri kullanım yoğunluğuna göre istatistiksel açıdan anlamlı düzeyde farklılık gösterip göstermediğinin belirlenmesi amacıyla ANOVA tekniğinden yararlanılmıştır.

Çizelge 4.25. Bilgi sistemleri kullanılma yoğunluğu ANOVA sonuçları

	Grup	Frekans (f)	Ortalama	Oran (%)	Standart Sapma
Kurumun İş Süreçlerinde Bilgi Sistemlerinin Kullanılma Yoğunluğu	Çok Düşük	8	3,7474	74,80	0,42716
	Düşük	15	3,5764	71,40	0,50553
	Orta	22	3,5644	71,20	0,61677
	Yüksek	44	3,9295	78,40	0,49548
	Çok Yüksek	32	4,2637	85,20	0,50967
	Total	121	3,8957	77,80	0,57703

	Kareler Toplamı	Serbestlik Derecesi	Kareler Ortalaması	F	p
Gruplar Arası	8,503	4	2,126	7,84	<0,001
Grup İçi	31,453	116	0,271		
Toplam	39,956	120			

Çizelge 4.25'te; kurumun iş süreçlerinde bilgi sistemlerinin kullanılma yoğunluğu grupları, her grup için ankete kaç katılımcının yer aldığını gösteren frekans değeri, katılımcılar tarafından verilen cevapların katsayı ortalamaları, standart sapma değerleri, kareler toplamı, serbestlik derecesi, kareler ortalaması, test istatistiği (F değeri) ve anlamlılık değeri (p) verilmiştir.

Çizelge 4.25'teki frekans değerlerine bakılacak olursa, ankete kurumun iş süreçlerinde bilgi sistemlerinin kullanılma yoğunluğu çok düşük olan 8 katılımcı, düşük olan 15 katılımcı, orta olan 22 katılımcı, yüksek olan 44 katılımcı ve çok yüksek olan 32 katılımcının katılım sağladığı görülmektedir. Katılımcılar tarafından verilen cevapların katsayı ortalamaları değerlendirildiğinde, çok düşük olan grubun 3,7474, düşük olan grubun 3,5764, orta olan grubun 3,5644, yüksek olan grubun 3,9295 ve çok yüksek olan grubun 4,2637 ortalama katsayı değerlerine sahip olduğu ve yüzde oranlarının sırasıyla %74,80, %71,40, %71,20, %78,40 ve %85,20 olduğu görülmektedir. Çok düşük, düşük ve orta gruplarında kurumun iş süreçlerinde bilgi sistemlerinin kullanılma yoğunluğu düzeyi arttıkça katsayı ortalamaları değerlerinin sırasıyla artmadığı görülmektedir. Böylece kurumun iş süreçlerinde bilgi sistemlerinin kullanılma yoğunluğu düzeyi arttıkça bilgi güvenliği politikalarının

etkinliğinin her zaman arttığı söylenemez. Ancak orta düzeyden itibaren kurumun iş süreçlerinde bilgi sistemlerinin kullanılma yoğunluğu düzeyi arttıkça katsayı ortalamaları değerleri arttığı için bilgi güvenliği politikalarının etkinliğinin arttığı söylenebilir.

Çizelge 4.25'te görüldüğü üzere p anlamlılık değeri <0,001 olarak hesaplanmıştır. Bu durumda p<0,05 olduğu için gruplar arasında istatistiki açıdan anlamlı farklılıklar bulunduğu belirlenmiştir. Hangi gruplar arasında anlamlı farklılıklar bulunduğuna ilişkin bilgiler Çizelge 4.26'da verilmiştir.

Böylece "*H1b: Kamu kurumlarının iş süreçlerinde bilgi sistemleri kullanım yoğunluğu ile bilgi güvenliği politikalarının etkinliği arasında istatistiksel açıdan anlamlı düzeyde bir farklılık bulunmaktadır."* hipotezi kabul edilmiştir.

Çizelge 4.26. Bilgi sistemleri kullanılma yoğunluğu Tukey HSD sonuçları

Kurumun İş Süreçlerinde Bilgi Sistemleri Kullanılma Yoğunluğu		Ortalama Fark	p
Çok Düşük	Düşük	0,17101	0,944
	Orta	0,18300	0,914
	Yüksek	-0,18205	0,893
	Çok Yüksek	-0,51628	0,096
Düşük	Çok Düşük	-0,17101	0,944
	Orta	0,01199	1,000
	Yüksek	-0,35306	0,163
	Çok Yüksek	-,68728*	0,000
Orta	Çok Düşük	-0,18300	0,914
	Düşük	-0,01199	1,000
	Yüksek	-0,36506	0,062
	Çok Yüksek	-,69928*	0,000
Yüksek	Çok Düşük	0,18205	0,893
	Düşük	0,35306	0,163
	Orta	0,36506	0,062
	Çok Yüksek	-0,33422	0,051
Çok Yüksek	Çok Düşük	0,51628	0,096
	Düşük	,68728*	0,000
	Orta	,69928*	0,000
	Yüksek	0,33422	0,051

Çizelge 4.26'ya bakılacak olursa, düşük ile çok yüksek grubu ve orta ile çok yüksek grubu için p değeri 0,000 olduğu görülmekte ve p<0,05 olduğu için ikişerli gruplar arasında anlamlı farklılık olduğu değerlendirilmektedir. Diğer grup eşleştirmeleri için p<0,05 şartı sağlanmadığı için anlamlı farklılık bulunmamaktadır. Örneğin yüksek ile çok yüksek grubu için p değeri 0,051 olduğu görülmekte, böylece iki grup arasında anlamlı farklılık olmadığı değerlendirilmektedir. Çizelge 4.26'da anlamlı farklılık olan gruplar * işareti ile ifade edilmiştir.

Çalışmanın temel amacı doğrultusunda belirlenen 17 alt ana başlık kapsamında oluşturulmuş olan sorulara yönelik elde edilen bulgulardan, kurumların iş süreçlerinde bilgi sistemleri kullanım yoğunluğu bağımsız değişkenine göre anlamlı farklılık gösterenler; bu bölümde çizelgeler halinde alt ana başlığı ve alt ana başlığına ilişkin sorular ifade edilmek üzere belirtilmiştir. Söz konusu sorulara yönelik elde edilen verilerden, bağımsız değişkenin grupları arasında anlamlı farklılık gösterenler çizelgelerde * işareti ile ifade edilmiştir. Anlamlı farklılık gösteren sorulara ilişkin kurumların iş süreçlerinde bilgi sistemleri kullanım yoğunluğu bağımsız değişkeninin grupları arasında kareler toplamı, serbestlik derecesi, kareler ortalaması, test istatistiği (F değeri) ve anlamlılık değeri (p) verilmiştir.

Çizelge 4.27'de "Bilgi Güvenliği Organizasyonu ve Sorumluluklar" alt ana başlığında yer alan "*Yönetim, bilgi sisteminin kurum amaçlarına uygun çalışmasını ve işlevlerini doğru bir şekilde yerine getirmesini sağlayacak tedbirleri almaktadır."* sorusuna ilişkin p değerinin 0,022 olduğu görülmekte ve dolayısıyla p<0,05 olduğu için bağımsız değişkenin grupları arasında anlamlı farklılıklar olduğunu söylemek mümkündür. Anlamlı olarak farklılık bulunan grup eşleştirmeleri için ortalama fark değerlerine bakılacak olursa çok düşük grubunun sırasıyla çok yüksek grubu ile 2,93750, yüksek grubu ile 2,43182, orta grubu ile 1,84091 ve düşük grubu ile 0,55000 ortalama fark değerlerinin büyükten küçüğe doğru sıralandığı görülmektedir. Böylece çok düşük grup ile çok yüksek grup arasındaki ortalama fark değeri, diğer gruplar arası karşılaştırma sonuç değerlerinden daha yüksek olduğu için bu iki grup arasındaki farklılık düzeyinin diğerlerinden daha anlamlı olduğu değerlendirilmektedir. *"Yürütülen çalışmalarda görevler ayrılığı ilkesine uygun davranılmaktadır."* ve "*İş süreçlerinde görevler ayrılığı ilkesinin uygulanabilmesi için yeterli sayıda ve nitelikte personel bulunmaktadır."* soruları için p değerinin 0,000 olduğu görülmekte ve dolayısıyla p<0,05 olduğu için bağımsız değişkenin grupları arasında anlamlı farklılıklar olduğunu söylemek mümkündür. Her iki soru için de anlamlı olarak farklılık

bulunan grup eşleştirmeleri için ortalama fark değerlerine bakılacak olursa çok düşük grubunun sırasıyla çok yüksek grubu ile 2,46875, yüksek grubu ile 2,09091, orta grubu ile 1,65909 ve düşük grubu ile 0,55000 ortalama fark değerlerinin büyükten küçüğe doğru sıralandığı görülmektedir. "*Bilgi güvenliğinin sağlanması açısından en az yetki ve bilmesi gereken prensibine uygun hareket edilmektedir."* sorusuna ilişkin p değerinin 0,035 olduğu görülmekte ve dolayısıyla $p<0,05$ olduğu için bağımsız değişkenin grupları arasında anlamlı farklılıklar olduğunu söylemek mümkündür. Anlamlı olarak farklılık bulunan grup eşleştirmeleri için ortalama fark değerlerine bakılacak olursa çok düşük grup ile çok yüksek grup arasında 0,86364 ortalama fark değerinin olduğu görülmektedir.

Çizelge 4.27. Bilgi güvenliği organizasyonu ve sorumluluklar için analiz sonuçları

Yönetim, bilgi sisteminin kurum amaçlarına uygun çalışmasını ve işlevlerini doğru bir şekilde yerine getirmesini sağlayacak tedbirleri almaktadır.	Grup	Çok Düşük	Düşük	Orta	Yüksek	Çok Yüksek
	Çok Düşük	-	-0,55000	-1,84091*	-2,43182*	-2,93750*
	Düşük	0,55000	-	-1,29091*	-1,88182*	-2,38750*
	Orta	1,84091*	1,29091*	-	-0,59091	-1,09659*
	Yüksek	2,43182*	1,88182*	0,59091	-	-0,50568
	Çok Yüksek	2,93750*	2,38750*	1,09659*	0,50568	-

	Kareler Toplamı	Serbestlik Derecesi	Kareler Ortalaması	F	p
Gruplar Arası	7,294	4	1,823	2,978	0,022
Grup İçi	71,037	116	0,612		
Toplam	78,331	120			

Yürütülen çalışmalarda görevler ayrılığı ilkesine uygun davranılmaktadır.	Grup	Çok Düşük	Düşük	Orta	Yüksek	Çok Yüksek
	Çok Düşük	-	-0,55000	-1,65909*	-2,09091*	-2,46875*
	Düşük	0,55000	-	-1,29091*	-1,88182*	-2,38750*
	Orta	1,84091*	1,29091*	-	-0,59091	-1,09659*
	Yüksek	2,43182*	1,88182*	0,59091	-	-0,50568
	Çok Yüksek	2,93750*	2,38750*	1,09659*	0,50568	-

	Kareler Toplamı	Serbestlik Derecesi	Kareler Ortalaması	F	p
Gruplar Arası	99,927	4	24,982	32,149	0,000
Grup İçi	90,139	116	0,777		
Toplam	190,066	120			

İş süreçlerinde görevler ayrılığı ilkesinin uygulanabilmesi için yeterli sayıda ve nitelikte personel bulunmaktadır.	Grup	Çok Düşük	Düşük	Orta	Yüksek	Çok Yüksek
	Çok Düşük	-	-0,55000	-1,65909*	-2,09091*	-2,46875*
	Düşük	0,55000	-	-1,10909*	-1,54091*	-1,91875*
	Orta	1,65909*	1,10909*	-	-0,43182	-,80966*
	Yüksek	2,09091*	1,54091*	0,43182	-	-0,37784
	Çok Yüksek	2,46875*	1,91875*	,80966*	0,37784	-

	Kareler Toplamı	Serbestlik Derecesi	Kareler Ortalaması	F	p
Gruplar Arası	67,794	4	16,949	16,938	0,000
Grup İçi	116,073	116	1,001		
Toplam	183,868	120			

Bilgi güvenliğinin sağlanması açısından en az yetki ve bilmesi gereken prensibine uygun hareket edilmektedir.	Grup	Çok Düşük	Düşük	Orta	Yüksek	Çok Yüksek
	Çok Düşük	-	0,65000	1,11364	0,52273	0,25000
	Düşük	-0,65000	-	0,46364	-0,12727	-0,40000
	Orta	-1,11364	-0,46364	-	-0,59091	-,86364*
	Yüksek	-0,52273	0,12727	0,59091	-	-0,27273
	Çok Yüksek	-0,25000	0,40000	,86364*	0,27273	-

	Kareler Toplamı	Serbestlik Derecesi	Kareler Ortalaması	F	p
Gruplar Arası	12,458	4	3,114	2,688	0,035
Grup İçi	134,418	116	1,159		
Toplam	146,876	120			

Çizelge 4.28'de "Farkındalık ve Eğitim" alt ana başlığında yer alan *"Gerçekleştirilen bilgi güvenliği farkındalık çalışmaları yeterli ve amacına uygundur."* sorusuna ilişkin p değerinin 0,035 olduğu görülmekte ve dolayısıyla p<0,05 olduğu için bağımsız değişkenin grupları arasında anlamlı farklılıklar olduğunu söylemek mümkündür. Anlamlı olarak farklılık bulunan grup eşleştirmeleri için ortalama fark değerlerine bakılacak olursa çok düşük grup ile orta grup arasında 1,17045 ortalama fark değerinin olduğu görülmekte*dir. "Yönetim, bilgi teknolojileri alanında çalışan ve bilgi güvenliği organizasyonunda yer alan personelin güncel bilgi güvenliği konularından haberdar olması adına personel gelişimini destekleyici tutum ve davranışlar ortaya koymaktadır."* sorusuna ilişkin p değerinin 0,000 olduğu görülmekte ve dolayısıyla p<0,05 olduğu için bağımsız değişkenin grupları arasında anlamlı farklılıklar olduğunu söylemek mümkündür. Anlamlı olarak farklılık bulunan grup eşleştirmeleri için ortalama fark değerlerine bakılacak olursa çok düşük grubunun sırasıyla çok yüksek grubu ile 2,43750, yüksek grubu ile 2,20455, orta grubu ile 1,65909 ve düşük grubu ile 0,68333 ortalama fark değerlerinin büyükten küçüğe doğru sıralandığı görülmektedir.

Çizelge 4.28. Farkındalık ve eğitim başlığı için analiz sonuçları

Gerçekleştirilen bilgi güvenliği farkındalık çalışmaları yeterli ve amacına uygundur.	Grup	Çok Düşük	Düşük	Orta	Yüksek	Çok Yüksek
	Çok Düşük	-	0,45833	1,17045*	0,53409	0,50000
	Düşük	0,45833	-	0,71212	0,07576	0,04167
	Orta	-1,17045*	-0,71212	-	-0,63636	-0,67045
	Yüksek	-0,53409	-0,07576	0,63636	-	-0,03409
	Çok Yüksek	-0,50000	-0,04167	0,67045	0,03409	-

	Kareler Toplamı	Serbestlik Derecesi	Kareler Ortalaması	F	p
Gruplar Arası	10,850	4	2,712	2,682	0,035
Grup İçi	117,299	116	1,011		
Toplam	128,149	120			

Yönetim, bilgi teknolojileri alanında çalışan ve bilgi güvenliği organizasyonunda yer alan personelin güncel bilgi güvenliği konularından haberdar olması adına personel gelişimini destekleyici tutum ve davranışlar ortaya koymaktadır.	Grup	Çok Düşük	Düşük	Orta	Yüksek	Çok Yüksek
	Çok Düşük	-	-0,68333	-1,65909*	-2,20455*	-2,43750*
	Düşük	-0,68333	-	-,97576*	-1,52121*	-1,75417*
	Orta	1,65909*	,97576*	-	-0,54545	-,77841*
	Yüksek	2,20455*	1,52121*	0,54545	-	-0,23295
	Çok Yüksek	2,43750*	1,75417*	,77841*	0,23295	-

	Kareler Toplamı	Serbestlik Derecesi	Kareler Ortalaması	F	p
Gruplar Arası	65,138	4	16,284	19,269	0,000
Grup İçi	98,036	116	0,845		
Toplam	163,174	120			

Çizelge 4.29'da "Varlık Yönetimi" alt ana başlığında yer alan *"Sahip olunan bilgi varlıklarına ilişkin envanter tutulmaktadır ve güncelliği sağlanmaktadır."* sorusuna ilişkin p değerinin 0,000 olduğu görülmekte ve dolayısıyla $p<0,05$ olduğu için bağımsız değişkenin grupları arasında anlamlı farklılıklar olduğunu söylemek mümkündür. Anlamlı olarak farklılık bulunan grup eşleştirmeleri için ortalama fark değerlerine bakılacak olursa çok düşük grubunun sırasıyla çok yüksek grubu ile 2,68750, yüksek grubu ile 2,70455, orta grubu ile 1,70455 ve düşük grubu ile 0,68333 ortalama fark değerlerinin büyükten küçüğe doğru sıralandığı görülmektedir.

Çizelge 4.29. Varlık yönetimi başlığı için analiz sonuçları

Sahip olunan bilgi varlıklarına ilişkin envanter tutulmaktadır ve güncelliği sağlanmaktadır.	Grup	Çok Düşük	Düşük	Orta	Yüksek	Çok Yüksek
	Çok Düşük	-	-0,68333	-1,70455*	-2,70455*	-2,68750*
	Düşük	-0,68333	-	-1,02121*	-2,02121*	-2,00417*
	Orta	1,70455*	1,02121*	-	-1,00000*	-,98295*
	Yüksek	2,70455*	2,02121*	1,00000*	-	-0,01705
	Çok Yüksek	2,68750*	2,00417*	,98295*	-0,01705	-

	Kareler Toplamı	Serbestlik Derecesi	Kareler Ortalaması	F	p
Gruplar Arası	95,935	4	23,984	37,010	0,000
Grup İçi	75,172	116	0,648		
Toplam	171,107	120			

Çizelge 4.30'da "Risk Yönetimi" alt ana başlığında yer ala*n "Sahip olunan bilgi varlıklarına ilişkin etkin bir risk değerlendirme çalışması yapılmaktadır."* sorusuna ilişkin p değerinin 0,000 olduğu görülmekte ve dolayısıyla p<0,05 olduğu için bağımsız değişkenin grupları arasında anlamlı farklılıklar olduğunu söylemek mümkündür. Anlamlı olarak farklılık bulunan grup eşleştirmeleri için ortalama fark değerlerine bakılacak olursa çok düşük grubunun sırasıyla çok yüksek grubu ile 2,46875, yüksek grubu ile 2,45455, orta grubu ile 1,88636 ve düşük grubu ile 0,48333 ortalama fark değerlerinin büyükten küçüğe doğru sıralandığı görülmektedir. *"Risklere karşı tanımlanan düzeltici ve iyileştirici faaliyetler yeterli seviyededir."* sorusuna ilişkin p değerinin 0,029 olduğu görülmekte ve dolayısıyla p<0,05 olduğu için bağımsız değişkenin grupları arasında anlamlı farklılıklar olduğunu söylemek mümkündür. Anlamlı olarak farklılık bulunan grup eşleştirmeleri için ortalama fark değerlerine bakılacak olursa çok düşük grup ile orta grup arasında 1,15909 ortalama fark değerinin olduğu görülmektedir.

Çizelge 4.30. Risk yönetimi başlığı için analiz sonuçları

Sahip olunan bilgi varlıklarına ilişkin etkin bir risk değerlendirme çalışması yapılmaktadır.	Grup	Çok Düşük	Düşük	Orta	Yüksek	Çok Yüksek
	Çok Düşük	-	-0,48333	-1,88636*	-2,45455*	-2,46875*
	Düşük	-0,48333	-	-1,40303*	-1,97121*	-1,98542*
	Orta	1,88636*	1,40303*	-	-0,56818	-0,58239
	Yüksek	2,45455*	1,97121*	0,56818	-	0,01420
	Çok Yüksek	2,46875*	1,98542*	0,58239	0,01420	-

	Kareler Toplamı	Serbestlik Derecesi	Kareler Ortalaması	F	p
Gruplar Arası	82,588	4	20,647	28,977	0,000
Grup İçi	82,652	116	0,713		
Toplam	165,240	120			

Risklere karşı tanımlanan düzeltici ve iyileştirici faaliyetler yeterli seviyededir.	Grup	Çok Düşük	Düşük	Orta	Yüksek	Çok Yüksek
	Çok Düşük	-	0,58333	1,15909*	0,61364	0,59375
	Düşük	0,58333	-	0,57576	0,03030	0,01042
	Orta	-1,15909*	-0,57576	-	-0,54545	-0,56534
	Yüksek	-0,61364	-0,03030	0,54545	-	0,01989
	Çok Yüksek	-0,59375	-0,01042	0,56534	0,01989	-

	Kareler Toplamı	Serbestlik Derecesi	Kareler Ortalaması	F	p
Gruplar Arası	9,287	4	2,322	2,804	0,029
Grup İçi	96,052	116	0,828		
Toplam	105,339	120			

Çizelge 4.31'de "Parola Güvenliği" alt ana başlığında yer ala*n "Sahip olunan bilgi varlıklarına ilişkin etkin bir risk değerlendirme çalışması yapılmaktadır."* sorusuna ilişkin p değerinin 0,035 olduğu görülmekte ve dolayısıyla p<0,05 olduğu için bağımsız değişkenin grupları arasında anlamlı farklılıklar olduğunu söylemek mümkündür. Anlamlı olarak farklılık bulunan grup eşleştirmeleri için ortalama fark değerlerine bakılacak olursa çok yüksek grup ile orta grup arasında 0,58239 ortalama fark değerinin olduğu görülmektedir.

Çizelge 4.31. Parola güvenliği başlığı için analiz sonuçları

Sahip olduğum kullanıcı adı ve parola gibi bilgilerin gizliliği tarafımca yeterli bir şekilde sağlanmaktadır.	Grup	Çok Düşük	Düşük	Orta	Yüksek	Çok Yüksek
	Çok Düşük	-	0,30000	0,36364	0,13636	-0,21875
	Düşük	0,30000	-	0,06364	-0,16364	-0,51875
	Orta	-0,36364	-0,06364	-	-0,22727	-,58239*
	Yüksek	-0,13636	0,16364	0,22727	-	0,35511
	Çok Yüksek	0,21875	0,51875	,58239*	0,35511	-

	Kareler Toplamı	Serbestlik Derecesi	Kareler Ortalaması	F	p
Gruplar Arası	5,516	4	1,379	2,682	0,035
Grup İçi	59,641	116	0,514		
Toplam	65,157	120			

Çizelge 4.32'de "Ağ, Sistem ve Erişim Güvenliği" alt ana başlığında yer alan *"Kurum ağına bağlı sahip olduğum cihazlarda antivirüs programı çalışmaktadır."* sorusuna ilişkin p

değerinin 0,035 olduğu görülmekte ve dolayısıyla p<0,05 olduğu için bağımsız değişkenin grupları arasında anlamlı farklılıklar olduğunu söylemek mümkündür. Anlamlı olarak farklılık bulunan grup eşleştirmeleri için ortalama fark değerlerine bakılacak olursa çok yüksek grup ile orta grup arasında 0,57670 ortalama fark değerinin olduğu görülmektedir. *"Yetkisiz erişimler de dahil olmak üzere iç ağı, dış tehditlerden korumak için güvenlik önlemleri (güvenlik duvarı vb.) alınmaktadır."* sorusuna ilişkin p değerinin 0,018 olduğu görülmekte ve dolayısıyla p<0,05 olduğu için bağımsız değişkenin grupları arasında anlamlı farklılıklar olduğunu söylemek mümkündür. Anlamlı olarak farklılık bulunan grup eşleştirmeleri için ortalama fark değerlerine bakılacak olursa çok yüksek grup ile orta grup arasında 0,56534 ortalama fark değerinin olduğu görülmektedir. *"Kritik sistemlere erişimde çoklu kimlik/çok faktörlü doğrulama mekanizmaları (MFA, 2FA) kullanılmaktadır."* sorusuna ilişkin p değerinin 0,000 olduğu görülmekte ve dolayısıyla p<0,05 olduğu için bağımsız değişkenin grupları arasında anlamlı farklılıklar olduğunu söylemek mümkündür. Anlamlı olarak farklılık bulunan grup eşleştirmeleri için ortalama fark değerlerine bakılacak olursa çok düşük grubunun sırasıyla çok yüksek grubu ile 3,00000, yüksek grubu ile 2,31818, orta grubu ile 1,70455 ve düşük grubu ile 0,55000 ortalama fark değerlerinin büyükten küçüğe doğru sıralandığı görülmektedir. *"Son kullanıcı aktiviteleri (log, denetim izi) güvenlik zafiyetleri ve bilgi sızdırmalarına karşı kayıt altına alınmaktadır."* sorusuna ilişkin p değerinin 0,007 olduğu görülmekte ve dolayısıyla p<0,05 olduğu için bağımsız değişkenin grupları arasında anlamlı farklılıklar olduğunu söylemek mümkündür. Anlamlı olarak farklılık bulunan grup eşleştirmeleri için ortalama fark değerlerine bakılacak olursa çok yüksek grubu ile yüksek ve orta grupları arasında 0,63920 ortalama fark değerinin olduğu görülmektedir. *"Kurum ağına uzaktan erişim yalnızca güvenli uzaktan bağlantı sağlayan sistemler (VPN vb.) üzerinden gerçekleştirilmektedir."* sorusuna ilişkin p değerinin 0,000 olduğu görülmekte ve dolayısıyla p<0,05 olduğu için bağımsız değişkenin grupları arasında anlamlı farklılıklar olduğunu söylemek mümkündür. Anlamlı olarak farklılık bulunan grup eşleştirmeleri için ortalama fark değerlerine bakılacak olursa çok düşük grubunun sırasıyla çok yüksek grubu ile 3,40625, yüksek grubu ile 3,11364, orta grubu ile 2,06818 ve düşük grubu ile 0,55000 ortalama fark değerlerinin büyükten küçüğe doğru sıralandığı görülmektedir. *"Kurum ağının saldırılara karşı korunabilmesi için gerekli güvenlik çözümleri (IPS, IDS, DDoS, WAF vb.) kullanılmaktadır."* sorusuna ilişkin p değerinin 0,003 olduğu görülmekte ve dolayısıyla p<0,05 olduğu için bağımsız değişkenin grupları arasında anlamlı farklılıklar olduğunu söylemek mümkündür. Anlamlı olarak farklılık bulunan grup eşleştirmeleri için ortalama fark değerlerine bakılacak olursa çok

yüksek grubu ile orta grup arasında 0,59659, yüksek grup arasında 0,57386 ortalama fark değerinin olduğu görülmektedir. *"Düzenli olarak sızma testi ve güvenlik denetimleri gerçekleştirilmektedir."* sorusuna ilişkin p değerinin 0,000 olduğu görülmekte ve dolayısıyla $p<0,05$ olduğu için bağımsız değişkenin grupları arasında anlamlı farklılıklar olduğunu söylemek mümkündür. Anlamlı olarak farklılık bulunan grup eşleştirmeleri için ortalama fark değerlerine bakılacak olursa çok düşük grubunun sırasıyla çok yüksek grubu ile 2,93750, yüksek grubu ile 2,32955, orta grubu ile 1,67045 ve düşük grubu ile 0,35833 ortalama fark değerlerinin büyükten küçüğe doğru sıralandığı görülmektedir.

Çizelge 4.32. Ağ, sistem ve erişim güvenliği başlığı için analiz sonuçları

Kurum ağına bağlı sahip olduğum cihazlarda antivirüs programı çalışmaktadır.	Grup	Çok Düşük	Düşük	Orta	Yüksek	Çok Yüksek
	Çok Düşük	-	-0,02500	0,42045	0,07955	-0,15625
	Düşük	-0,02500	-	0,44545	0,10455	-0,13125
	Orta	-0,42045	-0,44545	-	-0,34091	-,57670*
	Yüksek	-0,07955	-0,10455	0,34091	-	0,23580
	Çok Yüksek	0,15625	0,13125	,57670*	0,23580	-

	Kareler Toplamı	Serbestlik Derecesi	Kareler Ortalaması	F	p
Gruplar Arası	7,552	4	1,888	2,690	0,035
Grup İçi	81,407	116	0,702		
Toplam	88,959	120			

Yetkisiz erişimler de dahil olmak üzere iç ağı, dış tehditlerden korumak için güvenlik önlemleri (güvenlik duvarı vb.) alınmaktadır.	Grup	Çok Düşük	Düşük	Orta	Yüksek	Çok Yüksek
	Çok Düşük	-	0,43333	0,40909	0,22727	-0,15625
	Düşük	0,43333	-	-0,02424	-0,20606	-0,58958
	Orta	-0,40909	0,02424	-	-0,18182	-,56534*
	Yüksek	-0,22727	0,20606	0,18182	-	0,38352
	Çok Yüksek	0,15625	0,58958	,56534*	0,38352	-

	Kareler Toplamı	Serbestlik Derecesi	Kareler Ortalaması	F	p
Gruplar Arası	6,079	4	1,520	3,109	0,018
Grup İçi	56,698	116	0,489		
Toplam	62,777	120			

Kritik sistemlere erişimde çoklu kimlik/çok faktörlü doğrulama mekanizmaları (MFA, 2FA) kullanılmaktadır.	Grup	Çok Düşük	Düşük	Orta	Yüksek	Çok Yüksek
	Çok Düşük	-	-0,55000	-1,70455*	-2,31818*	-3,00000*
	Düşük	-0,55000	-	-1,15455*	-1,76818*	-2,45000*
	Orta	1,70455*	1,15455*	-	-0,61364	-1,29545*
	Yüksek	2,31818*	1,76818*	0,61364	-	,68182*
	Çok Yüksek	3,00000*	2,45000*	1,29545*	,68182*	-

	Kareler Toplamı	Serbestlik Derecesi	Kareler Ortalaması	F	p
Gruplar Arası	101,887	4	25,472	26,947	0,000
Grup İçi	109,650	116	0,945		
Toplam	211,537	120			

Son kullanıcı aktiviteleri (log, denetim izi) güvenlik zafiyetleri ve bilgi sızdırmalarına karşı kayıt altına alınmaktadır.	Grup	Çok Düşük	Düşük	Orta	Yüksek	Çok Yüksek
	Çok Düşük	-	0,24167	0,42045	0,42045	-0,21875
	Düşük	0,24167	-	0,17879	0,17879	-0,46042
	Orta	-0,42045	-0,17879	-	0,00000	-,63920*
	Yüksek	-0,42045	-0,17879	0,00000	-	,63920*
	Çok Yüksek	0,21875	0,46042	,63920*	,63920*	-

	Kareler Toplamı	Serbestlik Derecesi	Kareler Ortalaması	F	p
Gruplar Arası	9,165	4	2,291	3,682	0,007
Grup İçi	72,191	116	0,622		
Toplam	81,355	120			

Çizelge 4.32. (devam) Ağ, sistem ve erişim güvenliği başlığı için analiz sonuçları

Kurum ağına uzaktan erişim yalnızca güvenli uzaktan bağlantı sağlayan sistemler (VPN vb.) üzerinden gerçekleştirilmektedir.	Grup	Çok Düşük	Düşük	Orta	Yüksek	Çok Yüksek
	Çok Düşük	-	-0,55000	-2,06818*	-3,11364*	-3,40625*
	Düşük	-0,55000	-	-1,51818*	-2,56364*	-2,85625*
	Orta	2,06818*	1,51818*	-	-1,04545*	-1,33807*
	Yüksek	3,11364*	2,56364*	1,04545*	-	0,29261
	Çok Yüksek	3,40625*	2,85625*	1,33807*	0,29261	-

	Kareler Toplamı	Serbestlik Derecesi	Kareler Ortalaması	F	p
Gruplar Arası	153,927	4	38,482	82,552	0,000
Grup İçi	54,073	116	0,466		
Toplam	208,000	120			

Kurum ağının saldırılara karşı korunabilmesi için gerekli güvenlik çözümleri (IPS, IDS, DDoS, WAF vb.) kullanılmaktadır.	Grup	Çok Düşük	Düşük	Orta	Yüksek	Çok Yüksek
	Çok Düşük	-	0,36667	0,40909	0,38636	-0,18750
	Düşük	0,36667	-	0,04242	0,01970	-0,55417
	Orta	-0,40909	-0,04242	-	-0,02273	-,59659*
	Yüksek	-0,38636	-0,01970	0,02273	-	,57386*
	Çok Yüksek	0,18750	0,55417	,59659*	,57386*	-

	Kareler Toplamı	Serbestlik Derecesi	Kareler Ortalaması	F	p
Gruplar Arası	8,018	4	2,004	4,238	0,003
Grup İçi	54,858	116	0,473		
Toplam	62,876	120			

Düzenli olarak sızma testi ve güvenlik denetimleri gerçekleştirilmektedir.	Grup	Çok Düşük	Düşük	Orta	Yüksek	Çok Yüksek
	Çok Düşük	-	-0,35833	-1,67045*	-2,32955*	-2,93750*
	Düşük	-0,35833	-	-1,31212*	-1,97121*	-2,57917*
	Orta	1,67045*	1,31212*	-	-,65909*	-1,26705*
	Yüksek	2,32955*	1,97121*	,65909*	-	,60795*
	Çok Yüksek	2,93750*	2,57917*	1,26705*	,60795*	-

	Kareler Toplamı	Serbestlik Derecesi	Kareler Ortalaması	F	p
Gruplar Arası	107,625	4	26,906	40,119	0,000
Grup İçi	77,797	116	0,671		
Toplam	185,421	120			

Çizelge 4.33'te "Uygulama Güvenliği" alt ana başlığında yer alan *"Bağlantı yaptığım sistemde uzun süre aktif olmadığım durumda bağlantımın sona erdirilmesi için oturum zaman aşımı süresi çözümü uygulanmaktadır."* sorusuna ilişkin p değerinin 0,008 olduğu görülmekte ve dolayısıyla p<0,05 olduğu için bağımsız değişkenin grupları arasında anlamlı farklılıklar olduğunu söylemek mümkündür. Anlamlı olarak farklılık bulunan grup eşleştirmeleri için ortalama fark değerlerine bakılacak olursa çok yüksek grup ile orta grup arasında 0,73011 ortalama fark değerinin olduğu görülmektedir. "*Kurum bünyesinde geliştirilen uygulamalarda güvenli yazılım geliştirme yaşam döngüsü süreçleri ve modellerinden faydalanılmaktadır."* sorusuna ilişkin p değerinin 0,022 olduğu görülmekte ve dolayısıyla p<0,05 olduğu için bağımsız değişkenin grupları arasında anlamlı farklılıklar olduğunu söylemek mümkündür. Anlamlı olarak farklılık bulunan grup eşleştirmeleri için

ortalama fark değerlerine bakılacak olursa çok yüksek grup ile orta grup arasında 0,78977 ortalama fark değerinin olduğu görülmektedir.

Çizelge 4.33. Uygulama güvenliği başlığı için analiz sonuçları

Bağlantı yaptığım sistemde uzun süre aktif olmadığım durumda bağlantımın sona erdirilmesi için oturum zaman aşımı süresi çözümü uygulanmaktadır.	Grup	Çok Düşük	Düşük	Orta	Yüksek	Çok Yüksek
	Çok Düşük	-	0,36667	0,63636	0,29545	-0,09375
	Düşük	0,36667	-	0,26970	-0,07121	-0,46042
	Orta	-0,63636	-0,26970	-	-0,34091	-,73011*
	Yüksek	-0,29545	0,07121	0,34091	-	0,38920
	Çok Yüksek	0,09375	0,46042	,73011*	0,38920	-

	Kareler Toplamı	Serbestlik Derecesi	Kareler Ortalaması	F	p
Gruplar Arası	7,856	4	1,964	3,605	0,008
Grup İçi	63,202	116	0,545		
Toplam	71,058	120			

Kurum bünyesinde geliştirilen uygulamalarda güvenli yazılım geliştirme yaşam döngüsü süreçleri ve modellerinden faydalanılmaktadır.	Grup	Çok Düşük	Düşük	Orta	Yüksek	Çok Yüksek
	Çok Düşük	-	0,33333	0,72727	0,40909	-0,06250
	Düşük	0,33333	-	0,39394	0,07576	-0,39583
	Orta	-0,72727	-0,39394	-	-0,31818	-,78977*
	Yüksek	-0,40909	-0,07576	0,31818	-	0,47159
	Çok Yüksek	0,06250	0,39583	,78977*	0,47159	-

	Kareler Toplamı	Serbestlik Derecesi	Kareler Ortalaması	F	p
Gruplar Arası	9,478	4	2,369	2,981	0,022
Grup İçi	92,208	116	0,795		
Toplam	101,686	120			

Çizelge 4.34'te "İşletim Güvenliği" alt ana başlığında yer alan *"Bilgi güvenliğini etkileyen kurum iş süreçleri, bilgi işleme olanakları ve sistemlerdeki değişikliklere ilişkin planlama ve test çalışmaları yapılmaktadır."* sorusuna ilişkin p değerinin 0,000 olduğu görülmekte ve dolayısıyla p<0,05 olduğu için bağımsız değişkenin grupları arasında anlamlı farklılıklar olduğunu söylemek mümkündür. Anlamlı olarak farklılık bulunan grup eşleştirmeleri için ortalama fark değerlerine bakılacak olursa orta grup ile çok yüksek grup arasında 1,07670, yüksek grup arasında ,68182, düşük grup arasında 1,22121 ve çok düşük grup arasında 1,70455 ortalama fark değerinin olduğu görülmektedir. "*Yürütülen çalışmalarda bilgi güvenliği gereksinimleri için etkin bir test süreci işletilmektedir."* sorusuna ilişkin p değerinin 0,007 olduğu görülmekte ve dolayısıyla p<0,05 olduğu için bağımsız değişkenin grupları arasında anlamlı farklılıklar olduğunu söylemek mümkündür. Anlamlı olarak farklılık bulunan grup eşleştirmeleri için ortalama fark değerlerine bakılacak olursa orta grup

ile çok yüksek grup arasında 0,92898, yüksek grup arasında ,84091, çok düşük grup arasında 1,39773 ortalama fark değerinin olduğu görülmektedir.

Çizelge 4.34. İşletim güvenliği başlığı için analiz sonuçları

Bilgi güvenliğini etkileyen kurum iş süreçleri, bilgi işleme olanakları ve sistemlerdeki değişikliklere ilişkin planlama ve test çalışmaları yapılmaktadır.	Grup	Çok Düşük	Düşük	Orta	Yüksek	Çok Yüksek
	Çok Düşük	-	-0,48333	-1,70455*	-2,38636*	-2,78125*
	Düşük	-0,48333	-	-1,22121*	-1,90303*	-2,29792*
	Orta	1,70455*	1,22121*	-	-,68182*	-1,07670*
	Yüksek	2,38636*	1,90303*	,68182*	-	0,39489
	Çok Yüksek	2,78125*	2,29792*	1,07670*	0,39489	-

	Kareler Toplamı	Serbestlik Derecesi	Kareler Ortalaması	F	p
Gruplar Arası	94,437	4	23,609	38,825	0,000
Grup İçi	70,538	116	0,608		
Toplam	164,975	120			

Yürütülen çalışmalarda bilgi güvenliği gereksinimleri için etkin bir test süreci işletilmektedir.	Grup	Çok Düşük	Düşük	Orta	Yüksek	Çok Yüksek
	Çok Düşük	-	0,45833	1,39773*	0,55682	0,46875
	Düşük	0,45833	-	0,93939	0,09848	0,01042
	Orta	-1,39773*	-0,93939	-	-,84091*	-,92898*
	Yüksek	-0,55682	-0,09848	,84091*	-	0,08807
	Çok Yüksek	-0,46875	-0,01042	,92898*	0,08807	-

	Kareler Toplamı	Serbestlik Derecesi	Kareler Ortalaması	F	p
Gruplar Arası	17,645	4	4,411	3,746	0,007
Grup İçi	136,586	116	1,177		
Toplam	154,231	120			

Çizelge 4.35'te "Tedarikçi İlişkilerinde Bilgi Güvenliği" alt ana başlığında yer alan *"Tedarikçiler tarafından sağlanan hizmetlerde bilgi güvenliği riskleri oluşturabilecek durumlara karşı dikkatli davranılmaktadır."* sorusuna ilişkin p değerinin 0,025 olduğu görülmekte ve dolayısıyla $p<0,05$ olduğu için bağımsız değişkenin grupları arasında anlamlı farklılıklar olduğunu söylemek mümkündür. Anlamlı olarak farklılık bulunan grup eşleştirmeleri için ortalama fark değerlerine bakılacak olursa orta grup ile çok yüksek grup arasında ,76705 ortalama fark değerinin olduğu görülmektedir.

Çizelge 4.35. Tedarikçi ilişkilerinde bilgi güvenliği başlığı için analiz sonuçları

Tedarikçiler tarafından sağlanan hizmetlerde bilgi güvenliği riskleri oluşturabilecek durumlara karşı dikkatli davranılmaktadır.	Grup	Çok Düşük	Düşük	Orta	Yüksek	Çok Yüksek
	Çok Düşük	-	0,05000	0,70455	0,22727	-0,06250
	Düşük	0,05000	-	0,65455	0,17727	-0,11250
	Orta	-0,70455	-0,65455	-	-0,47727	-,76705*
	Yüksek	-0,22727	-0,17727	0,47727	-	0,28977
	Çok Yüksek	0,06250	0,11250	,76705*	0,28977	-

	Kareler Toplamı	Serbestlik Derecesi	Kareler Ortalaması	F	p
Gruplar Arası	8,496	4	2,124	2,891	0,025
Grup İçi	85,207	116	0,735		
Toplam	93,702	120			

Çizelge 4.36'da "Fiziksel Güvenlik" alt ana başlığında yer alan *"Belirli alanlara giriş ve çıkışlarda elektronik kapı, turnike, görüntü/ses kayıtları gibi fiziksel güvenlik önlemleri uygulanmaktadır."* sorusuna ilişkin p değerinin 0,005 olduğu görülmekte ve dolayısıyla $p<0,05$ olduğu için bağımsız değişkenin grupları arasında anlamlı farklılıklar olduğunu söylemek mümkündür. Anlamlı olarak farklılık bulunan grup eşleştirmeleri için ortalama fark değerlerine bakılacak olursa orta grup ile çok yüksek grup arasında 0,62216 ortalama fark değerinin olduğu görülmektedir.

Çizelge 4.36. Fiziksel güvenlik başlığı için analiz sonuçları

Belirli alanlara giriş ve çıkışlarda elektronik kapı, turnike, görüntü/ses kayıtları gibi fiziksel güvenlik önlemleri uygulanmaktadır.	Grup	Çok Düşük	Düşük	Orta	Yüksek	Çok Yüksek
	Çok Düşük	-	0,10833	0,46591	0,19318	-0,15625
	Düşük	0,10833	-	0,35758	0,08485	-0,26458
	Orta	-0,46591	-0,35758	-	-0,27273	-,62216*
	Yüksek	-0,19318	-0,08485	0,27273	-	0,34943
	Çok Yüksek	0,15625	0,26458	,62216*	0,34943	-

	Kareler Toplamı	Serbestlik Derecesi	Kareler Ortalaması	F	p
Gruplar Arası	7,494	4	1,874	3,886	0,005
Grup İçi	55,927	116	0,482		
Toplam	63,421	120			

Çizelge 4.37'de "İnsan Kaynakları Güvenliği" alt ana başlığında yer alan *"Bilgi varlıklarının amacına uygun kullanılmadığı durumlarda yaşanması muhtemel bilgi güvenliği ihlal olaylarından dolayı devreye girebilecek bir disiplin süreci oluşturulmuştur."* sorusuna ilişkin p değerinin 0,007 olduğu görülmekte ve dolayısıyla $p<0,05$ olduğu için bağımsız değişkenin grupları arasında anlamlı farklılıklar olduğunu söylemek mümkündür. Anlamlı olarak farklılık bulunan grup eşleştirmeleri için ortalama fark değerlerine bakılacak

olursa orta grup ile çok yüksek grup arasında 0,75284 ortalama fark değerinin olduğu görülmektedir.

Çizelge 4.37. İnsan kaynakları güvenliği başlığı için analiz sonuçları

Bilgi varlıklarının amacına uygun kullanılmadığı durumlarda yaşanması muhtemel bilgi güvenliği ihlal olaylarından dolayı devreye girebilecek bir disiplin süreci oluşturulmuştur.	Grup	Çok Düşük	Düşük	Orta	Yüksek	Çok Yüksek
	Çok Düşük	-	0,70833	0,78409	0,53409	0,03125
	Düşük	0,70833	-	0,07576	-0,17424	-0,67708
	Orta	-0,78409	-0,07576	-	-0,25000	-,75284*
	Yüksek	-0,53409	0,17424	0,25000	-	0,50284
	Çok Yüksek	-0,03125	0,67708	,75284*	0,50284	-

	Kareler Toplamı	Serbestlik Derecesi	Kareler Ortalaması	F	p
Gruplar Arası	10,963	4	2,741	3,713	0,007
Grup İçi	85,632	116	0,738		
Toplam	96,595	120			

Çizelge 4.38'de "Bilgi Güvenliği İhlal Olay Yönetimi" alt ana başlığında yer alan *"Bilgi güvenliği ihlal olaylarına zamanında ve uygun karşılık verilebilmektedir."* sorusuna ilişkin p değerinin 0,002 olduğu görülmekte ve dolayısıyla $p<0,05$ olduğu için bağımsız değişkenin grupları arasında anlamlı farklılıklar olduğunu söylemek mümkündür. Anlamlı olarak farklılık bulunan grup eşleştirmeleri için ortalama fark değerlerine bakılacak olursa orta grup ile çok yüksek grup arasında ,80966, çok düşük grup arasında ,96591 ortalama fark değerinin olduğu görülmektedir.

Çizelge 4.38. Bilgi güvenliği ihlal olay yönetimi başlığı için analiz sonuçları

Bilgi güvenliği ihlal olaylarına zamanında ve uygun karşılık verilebilmektedir.	Grup	Çok Düşük	Düşük	Orta	Yüksek	Çok Yüksek
	Çok Düşük	-	0,44167	,96591*	0,57955	0,15625
	Düşük	0,44167	-	0,52424	0,13788	-0,28542
	Orta	-,96591*	-0,52424	-	-0,38636	-,80966*
	Yüksek	-0,57955	-0,13788	0,38636	-	0,42330
	Çok Yüksek	-0,15625	0,28542	,80966*	0,42330	-

	Kareler Toplamı	Serbestlik Derecesi	Kareler Ortalaması	F	p
Gruplar Arası	10,849	4	2,712	4,447	0,002
Grup İçi	70,754	116	0,610		
Toplam	81,603	120			

5. SONUÇ VE ÖNERİLER

Kamu kurumlarının bilgi güvenliği çalışmaları kapsamında oluşturduğu bilgi güvenliği politikalarının etkinliğinin incelenmesi amacıyla yapılmış olan bu çalışmada, farklı kurumlarda çalışan katılımcılara uygulanan anket ile katılımcıların kurumlarının bilgi güvenliği politikalarında ele alınan temel hususların uygulamadaki etkinlik durumlarının kurumların yapılarına göre değişiklik gösterip göstermediği araştırılmıştır. Bu kapsamda çalışmada, kurumların sahip olduğu verilerin kritiklik düzeyi ve kurumların iş süreçlerinde bilgi sistemleri kullanım yoğunluğu bağımsız değişkenlerine göre bilgi güvenliği politikalarının etkinlik düzeyinin değişip değişmediği incelenmiştir.

Araştırma evrenini 17 kamu kurumu oluşturmaktadır. Bu kurumlardan uygun örneklem yöntemiyle seçilen 6 kamu kurumu araştırmanın örneklemini oluşturmaktadır. Seçilen örneklemin araştırma evrenini temsil edebilmesi açısından yaklaşık %35 gibi yüksek bir oranda örneklem üzerinde anket çalışması gerçekleştirilmiştir.

Çalışma, temel bilgi güvenliği konularının bütünsel olarak ve araştırma kapsamında belirlenen değişkenler bazında ele alınarak analiz gerçekleştirilen ilk çalışma olması ve yasa koyuculara ve bilgi güvenliği alanında düzenleme ve/veya denetleme yetkisine sahip olan ilgili otoritelere yürütecekleri çalışmalarda ışık tutması bakımından önemlidir.

Çalışma kapsamında gerçekleştirilen anket sonuçlarına uygulanan istatistiki analiz yöntemleri neticesinde elde edilen bulgulara dayanarak varılan araştırma sonuçları aşağıda açıklanmıştır.

Birinci araştırma sorusuna ilişkin elde edilen bulgular değerlendirildiğinde; seçilen örneklem kümesinde yer alan kamu kurumlarının bilgi güvenliği politikalarının %77,80 oranında etkin olduğu söylenebilmektedir. Ayrıca, en etkin olan güvenlik konularının %86,20 oranı ile e-posta güvenliği ve %85,80 oranı ile fiziksel güvenlik olduğu; en az etkin olan güvenlik konularının %66,00 oranı ile farkındalık ve eğitim ve %67,70 oranı ile risk yönetimi olduğu sonucuna varılmıştır.

Özdemir (2019) ve Kapanoğlu (2016) tarafından yapılan çalışmalarda da farkındalık ve eğitim konularının orta seviyede etkin olduğu sonucuna varıldığı ifade edilmektedir. Bu

bağlamda çalışma sonuçları (%66 oranında etkin) ile ilgili araştırma sonuçlarının uyumlu olduğu değerlendirilmektedir.

İkinci araştırma sorusuna ilişkin elde edilen bulgular değerlendirildiğinde; çok düşük, düşük, orta, yüksek ve çok yüksek grupları için bilgi güvenliği politikalarının etkinlik oranının sırasıyla %72,20, %73,40, %76,20, %78,20 ve %85,00 olduğu belirlenmiştir. Böylece kurumun sahip olduğu verilerin kritiklik düzeyi arttıkça, bilgi güvenliği politikalarının etkinliğinin arttığı söylenebilmektedir. Kurumun sahip olduğu verilerin kritiklik düzeyi açısından ele alındığında, çok düşük ile çok yüksek grubu ($p=0,017$), düşük ile çok yüksek grubu ($p=0,008$) ve orta ile çok yüksek grubu ($p=0,019$) arasında $p<0,05$ şartı sağlandığı için istatistiksel açıdan anlamlı farklılık olduğu belirlenmiştir. Söz konusu grup eşleştirmeleri için ortalama fark değerleri sırasıyla 0,64708, 0,58471 ve 0,44384 olarak hesaplanmıştır. Bu bağlamda çok düşük ile çok yüksek grubu arasındaki ortalama fark değerinin diğerlerinden daha yüksek olduğu için farklılık düzeyinin diğerlerinden daha anlamlı olduğu, benzer şekilde düşük ile çok yüksek grupları arasındaki farklılık düzeyinin de orta ile çok yüksek grupları arasındaki farklılık düzeyinden daha anlamlı olduğu sonucuna varılmıştır.

CB DDO tarafından yayımlanan Bilgi ve İletişim Güvenliği Rehberi'nde (2020) kurumların sahip oldukları varlık gruplarının kritik düzeylerine göre güvenlik tedbirleri seviyelendirilmiştir. Kritiklik düzeyi yüksek olan varlık gruplarına daha ileri seviyeli tedbirler uygulanması zorunlu tutulurken, düşük olanlar için daha düşük seviyedeki tedbirleri uygulanması zorunlu tutulmuştur. Bu bağlamda araştırma sonucunda; kurumun sahip olduğu verilerin kritiklik düzeyi arttıkça, bilgi güvenliği politikalarının etkinliğinin arttığı tespiti ile Rehber'de benimsenen yaklaşımın uyumlu olduğu değerlendirilmektedir.

Üçüncü araştırma sorusuna ilişkin elde edilen bulgular değerlendirildiğinde; çok düşük, düşük, orta, yüksek ve çok yüksek grupları için bilgi güvenliği politikalarının etkinlik oranının sırasıyla %74,80, %71,40, %71,20, %78,40 ve %85,20 olduğu belirlenmiştir. Böylece kurumun iş süreçlerinde bilgi sistemlerinin kullanılma yoğunluğu arttıkça, bilgi güvenliği politikalarının etkinliğinin her zaman arttığı söylenemez. Çünkü sonuçlardan görüldüğü üzere çok düşük, düşük ve orta grupları için etkinlik yüzdeleri bu kaideyi bozmaktadır. Ancak orta düzeyden itibaren, kurumun iş süreçlerinde bilgi sistemlerinin kullanılma yoğunluğu arttıkça, bilgi güvenliği politikalarının etkinliğinin arttığı söylenebilmektedir. Kurumun iş süreçlerinde bilgi sistemlerinin kullanılma yoğunluğu

açısından ele alındığında, düşük ile çok yüksek grubu (p=0,000) ve orta ile çok yüksek grubu (p=0,000) arasında p<0,05 şartı sağlandığı için istatistiksel açıdan anlamlı farklılık bulunduğu, diğer grup eşleştirmeleri için p<0,05 şartı sağlanmadığı için anlamlı farklılık bulunmadığı sonucuna varılmıştır.

Literatürde yer alan benzer çalışmalarda (Özdemir, 2019; Kapanoğlu, 2016; Solmaz, 2020; Tuygun, 2019; Henkoğlu, 2015; Çek, 2017; Şişkin, 2020; Vural, 2007) daha çok eğitim ve farkındalık faaliyetleri vb. ekseninde insan faktörlü etkiler üzerine odaklanıldığı görülmekteyken, bu çalışmada bilgi güvenliği politikalarında yer alan ağ ve sistem güvenliği, uygulama güvenliği, e-posta güvenliği, parola güvenliği, fiziksel güvenlik gibi temel güvenlik konularının kurumlar tarafından yerine getirilme durumu noktasında yürütülmüş olan çalışmalar ve bu doğrultuda kurumların hazırlamış oldukları bilgi güvenliği politikaları tüm yönleriyle ele alınmıştır.

Çalışma sonuçları; ilgili otoritelerce yapılan mevcut düzenlemelerin, atılan adımların ve alınan kararların ne derece yerinde, yeterli ve etkin olduğunun değerlendirilmesine katkı sağlamaktadır.

Araştırma sonuçlarına dayanarak ilgili araştırmacılara veya konuyla ilgilenen kişilere şu önerilerde bulunulabilir:

- Kurumların bilgi güvenliği politikalarının etkinlik değerlendirmeleri sonuçlarına göre kamu kurumlarına, araştırma ile etkinlik konusunda yetersiz olduğu ortaya çıkarılan bilgi güvenliği konularının etkinliğinin sağlanması için ilave çalışmalar yapmaları önerilmektedir.
- Kurumlarca bilgi güvenliği politikalarında ele alınan konuların bir kısmı etkin bir şekilde uygulanırken bir kısmının etkin bir şekilde uygulanmadığı görülmektedir. Politikaların etkin bir şekilde uygulanıp uygulanmadığının yetkili bir otorite tarafından denetlenmesinin politikaların etkin bir şekilde uygulanmasına katkı sağlayacağı düşünülmektedir. Cumhurbaşkanlığı Bilgi ve İletişim Güvenliği Tedbirleri Genelgesi'nde, kamu kurumlarının CB DDO tarafından çıkarılan Bilgi ve İletişim Güvenliği Rehberinde yer alan usul ve esaslara uymaları zorunlu tutulmuş olup kurumlar tarafından bu kapsamda gerçekleştirilen çalışmaların denetime tabi tutulacağı ifade edilmiştir. Araştırma kapsamında gerçekleştirilen anket çalışmasının, söz konusu

denetimlerin gerçekleştirilmesi sonrası tekrarlanması ve elde edilen sonuçların Rehber'in kurumların yürütmekte olduğu bilgi güvenliği çalışmalarına sağladığı katkıların değerlendirilmesi açısından karşılaştırılması önerilmektedir.

- Araştırmada bilgi güvenliği politikaları temel güvenlik konularını içerecek şekilde bütünsel olarak ele alınmıştır. Spesifik bir güvenlik konusuna ilişkin sonuçlar elde edilmek isteniyorsa, anketteki alt başlıklar nezdinde ayrıca bir araştırma yapılması önerilmektedir.
- Araştırmada uygulanan anketin, araştırma konusunda teknik ve mesleki bilgiye sahip katılımcılar üzerinde gerçekleştirilmesinin, daha anlamlı sonuçların elde edilmesine katkı sağladığı değerlendirilmektedir. Ancak ankete ilave olarak verilerin toplanması için görüşme tekniğinden faydalanılması önerilmektedir.

KAYNAKLAR

Acılar, A. (2009). İşletmelerde Bilgi Güvenliği ve Örgüt Kültürü. *Organizasyon ve Yönetim Bilimleri Dergisi*, 1(1), 25-33.

Aktaş, K. (2020). *ISO 27001 Bilgi Güvenliği Yönetim Sistemi: Erişim Kontrol Politikası Üzerine Bir İnceleme,* Yüksek Lisans Tezi, Doğuş Üniversitesi Lisansüstü Eğitim Enstitüsü, İstanbul.

Alqahtani, F. H. (2017). *Developing an Information Security Policy: A Case Study Approach.* 4th Information Systems International Conference. Indonesia, 691-697.

Alshaikh, M., Maynard, S., Ahmad, A., and Chang, S. (2015). *Information Security Policy: A Management Practice Perspective.* Australasian Conference on Information Systems. Adelaide South Australia.

Altınpulluk, Ö. (2016). *ISO 27001:2013 Bilgi Güvenliği Yönetim Sistemi Kurumsal Risk Yönetimi*, Yüksek Lisans Tezi, Yıldız Teknik Üniversitesi Fen Bilimleri Enstitüsü, İstanbul.

Angraini, Alias, R., and Okfalisa. (2019). *Information Security Policy Compliance: Systematic Literature Review.* The Fifth Information Systems International Conference. Surabaya, Indonesia, 1216-1224.

Ankara Üniversitesi. (2012, Şubat 26*). Evren, Örneklem, Örnekleme Türleri*. Ankara: Ankara Üniversitesi, 12.

Bakanlar Kurulu. (2012, Ekim 20). *Ulusal Siber Güvenlik Çalışmalarının Yürütülmesi, Yönetilmesi ve Koordinasyonuna İlişkin Karar*. Ankara: Bakanlar Kurulu, 2.

Başbakanlık. (2016, Aralık 3). *Kamu Kurum ve Kuruluşlarının KamuNet'e Dahil Edilmesi ile İlgili 2016/28 Sayılı Başbakanlık Genelgesi*. Ankara: Başbakanlık, 1.

Bhaharin, S., Mokhtar, U., Sulaiman, R., and Yusof, M. (2019). *Issues and Trends in Information Security Policy Compliance.* 2019 6th International Conference on Research and Innovation in Information Systems (ICRIIS). Malaysia.

Can, Ö., ve Akbaş, M. F. (2014). Kurumsal Ağ ve Sistem Güvenliği Politikalarının Önemi ve Bir Durum Çalışması. *Türk Bilim Araştırma Vakfı TUBAV Bilim Dergisi*, 7(2), 16-31.

Can, Ö., ve Ünalır, M. O. (2010). Ontoloji Tabanlı Bilgi Sistemlerinde Politika Yönetimi. *Gazi Üniversitesi Bilişim Enstitüsü Bilişim Teknolojileri Dergisi*, 3(2), 3.

Canbek, G., ve Sağıroğlu, Ş. (2006). Bilgi, Bilgi Güvenliği ve Süreçleri Üzerine Bir İnceleme. *Politeknik Dergisi*, 9(3), 165-174.

Cumhurbaşkanlığı. (2019, Temmuz 6). *Bilgi ve İletişim Güvenliği Tedbirleri Genelgesi*. Ankara: Cumhurbaşkanlığı, 1.

Cumhurbaşkanlığı Dijital Dönüşüm Ofisi Başkanlığı. (2020, Temmuz). *Bilgi ve İletişim Güvenliği Rehberi*. Ankara: Cumhurbaşkanlığı Dijital Dönüşüm Ofisi Başkanlığı, 1.

Cumhurbaşkanlığı Dijital Dönüşüm Ofisi Başkanlığı. (2022). *Elektronik Kamu Bilgi Yönetim Sistemi*. Ankara: Cumhurbaşkanlığı Dijital Dönüşüm Ofisi Başkanlığı, 1.

Çek, E. (2017). *Kurumsal Bilgi Güvenliği Yönetişimi ve Bilgi Güvenliği için İnsan Faktörünün Önemi*, Yüksek Lisans Tezi, İstanbul Bilgi Üniversitesi Sosyal Bilimler Enstitüsü, İstanbul.

Çetinkaya, M. (2008, Eylül). *Bilgi Güvenliği Yönetim Sistemi Alt Yapısının Değerlendirilmesi için Bir Test Aracı Geliştirilmesi,* Yüksek Lisans Tezi, İstanbul Kültür Üniversitesi Fen Bilimleri Enstitüsü, İstanbul.

Dayıoğlu, B. (2002). Ağ ve İşletim Sistemi Güvenliği. *Türkiye Bilişim Derneği 9. Bilgi İşlem Merkezi Yöneticileri Semineri (İMY9)*. Antalya, 30.

Disterer, G. (2013). ISO/IEC 27000, 27001 and 27002 for Information Security Management. *Journal of Information Security*. 92-100.

Earl, J. (2004). Controlling protest: New Directions For Research On The Social Control Of Protest. *Research in Social Movements, Conflicts and Change*. 55-83.

Ersoy, E. V. (2012). *ISO/IEC 27001 Bilgi Güvenliği Standardı Tanımlar ve Örnek Uygulamalar*. Ankara: ODTÜ Yayıncılık, 8.

Eskiyörük, D. (2008, Nisan 18). *Bilgi Sistemleri Kabul Edilebilir Kullanım Politikası Oluşturma Kılavuzu*. Kocaeli: Türkiye Bilimsel ve Teknolojik Araştırma Kurumu Ulusal Elektronik ve Kriptoloji Araştırma Enstitüsü, 9.

Gözel, S. (2020). *Bilgi ve İletişim Güvenliği Rehberi*. İstanbul: KPMG Türkiye Denetim, Vergi ve Danışmanlık Hizmetleri, 1.

Gurbetoğlu, A. (2018). *Bilimsel Araştırma Yöntemleri*. İstanbul: İstanbul Sabahattin Zaim Üniversitesi Eğitim Fakültesi, 8.

Henkoğlu, T. (2015). *Hassas Bilgi Varlıklarının ve Kişisel Verilerin Hukuksal Düzenlemeler ile Korunması ve Bu Kapsamda Üniversiteler İçin Bilgi Güvenliği Politikasının Geliştirilmesi,* Doktora Tezi, Hacettepe Üniversitesi Sosyal Bilimler Enstitüsü, Ankara.

Henkoğlu, T., ve Yılmaz, B. (2013). Avrupa Birliği (AB) Bilgi Güvenliği Politikaları. *Türk Kütüphaneciliği Dergisi*, 27(3), 451-471.

Hsu, C., Wang, T., and Lu, A. (2016). *The Impact of ISO 27001 Certification on Firm Performance.* 2016 49th Hawaii International Conference on System Sciences. 4842-4848.

InstantSecurityPolicy, (2010). *IT Security Policy Guide*. Durham: InstantSecurityPolicy, 6.

İftar, G. K. (1999). Bilim ve Araştırma. *Sosyal Bilimlerde Araştırma Yöntemleri*. Eskişehir: Anadolu Üniversitesi Yayınları, 7.

İslamoğlu, A., ve Alnıaçık, Ü. (2016). *Sosyal Bilimlerde Araştırma Yöntemleri*. İstanbul: Beta Yayınları, 146.

Kalman, S. (2003). *Web Security Field Guide*. Indianapolis: Cisco Press, 36-37.

Kapanoğlu, G. (2016, Eylül). *Öğretmenlerin Bilgi Güvenliği Farkındalığının İncelenmesi*, Yüksek Lisans Tezi, Gazi Üniversitesi Eğitim Bilimleri Enstitüsü, Ankara.

Karasar, N. (1999). *Bilimsel Araştırma Yöntemi*. Ankara: Nobel Yayın Dağıtım, 79.

Kılıç, B. (2019, Aralık). *ISO/IEC 27001 Bilgi Güvenliği Yönetim Sistemi Açısından Türkiye'de Hukuk Bürolarında Bilgi Güvenliği Yönetimi*, Yüksek Lisans Tezi, Gazi Üniversitesi Bilişim Enstitüsü, Ankara.

Kırışık, F., ve Sezer, Ö. (2015). Bilgi ve İletişim Teknolojilerinin (Bit) Kamu Politikası Oluşturma Sürecindeki Rolü. *Ekonomik ve Sosyal Araştırmalar Dergisi*, 11(2), 199-215.

KPMG Türkiye Denetim, Vergi ve Danışmanlık Hizmetleri. (2020). *Bilgi ve İletişim Güvenliği Rehberi*. İstanbul: KPMG Türkiye Denetim, Vergi ve Danışmanlık Hizmetleri, 1.

Luma, A., and Abazi, B. (2019). *The importance of integration of information security management systems (ISMS) to the organization's Enterprise Information Systems (EIS).* 2019 42nd International Convention on Information and Communication Technology, Electronics and Microelectronics (MIPRO). 1.

Mallery, P., and Darren, G. (2010). *2010 SPSS for Windows Step by Step: A Simple Guide and Reference 17.0 update*. Boston: Allyn & Bacon, 21.

Marttin, V., ve Pehlivan, İ. (2010). ISO 27001:2005 Bilgi Güvenliği Yönetimi Standardı ve Türkiye'deki Bazı Kamu Kuruluşu Uygulamaları Üzerine Bir İnceleme. *Mühendislik Bilimleri ve Tasarım Dergisi*, 49-56.

Metin, M. (2014). *Kuramdan Uygulamaya Eğitimde Bilimsel Araştırma Yöntemleri*. Ankara: Pegem Akademi, 2014, 163.

Nicho, M., and Muamaar, S. (2016). Towards a Taxonomy of Challenges in an Integrated IT Governance Framework Implementation. *Journal of International Technology and Information Management*. 1-31.

Odabaşı, Y. (1999). Anket Yöntemi. *Sosyal Bilimlerde Araştırma Yöntemleri*. Eskişehir: Anadolu Üniversitesi Yayınları, 81.

Onwubıko, C., and Lenaghan, A. (2007). *Managing Security Threats and Vulnerabilities for Small to Medium Enterprises.* 2007 IEEE International Conference on Intelligence and Security. New Brunswick, NJ, A.B.D, 244-249.

Özbek, Ç. (2012). *Kurumsal Yönetim-Risk Yönetimi-İç Kontrol* (Birinci Baskı). İstanbul: Türkiye İç Denetim Enstitüsü Yayınları, 1071.

Özbilen, T., ve Çağlar, A. (2020). Türk Kamu Sektöründe Bilgi ve Bilişim Güvenliği. *Kamu Yönetimi ve Teknoloji Dergisi (1)*, 72-93.

Özcan, B. (2009). *Kurumsal Bilgi Güvenliği ve COBIT*, Yüksek Lisans Tezi, Haliç Üniversitesi Fen Bilimleri Enstitüsü, İstanbul.

Özdemir, A. (2019, Aralık). *Kamu Kurum ve Kuruluşlarında Bilgi Güvenliği Farkındalığı*, Yüksek Lisans Tezi, Gazi Üniversitesi Bilişim Enstitüsü, Ankara.

Özmen, A. (1999). Örnekleme. *Sosyal Bilimlerde Araştırma Yöntemleri*. Eskişehir: Anadolu Üniversitesi Yayınları, 40.

Öztürk, G. (2008). *Bilgi Güvenliği Politikası Oluşturma Kılavuzu*. Kocaeli: Türkiye Bilimsel ve Teknolojik Araştırma Kurumu Ulusal Elektronik ve Kriptoloji Araştırma Enstitüsü, 9.

Solmaz, M. (2020, Nisan). *Öğretmen Adaylarının Siber Bilgi Güvenliği Farkındalıklarının ve Dijital Vatandaşlık Düzeylerinin Farklı Değişkenler Açısından İncelenmesi*, Yüksek Lisans Tezi, Mersin Üniversitesi Eğitim Bilimleri Enstitüsü, Mersin.

Szczepaniuk, E. K., Szczepaniuk, H., Rokicki, T., ve Klepacki, B. (2020). Information Security Assessment in Public Administration. *Computers & Security*. 3.

Şişkin, D. Ş. (2020). *Üniversite Kütüphanelerinde Bilgi Güvenliği ve Kişisel Verilerin Korunması: Ankara'daki Üniversite Kütüphanelerinin Değerlendirilmesi*, Yüksek Lisans Tezi, Hacettepe Üniversitesi Sosyal Bilimler Enstitüsü, Ankara.

Tekerek, M. (2008). Bilgi Güvenliği Yönetimi. *KSÜ Fen ve Mühendislik Dergisi*, 132-137.

Thakur, K., Ali, M., Gai, K., and Qiu, M. (2016). *Information Security Policy for E-Commerce in Saudi Arabia.* 2016 IEEE 2nd International Conference on Big Data Security on Cloud (BigDataSecurity), IEEE International Conference on High Performance and Smart Computing (HPSC), and IEEE International Conference on Intelligent Data and Security (IDS). 187-190.

The United Nations Economic and Social Commission for Asia and the Pacific. (2008). *Information Security for Economic and Social Development.* Bangkok: The United Nations Economic and Social Commission for Asia and the Pacific, 10.

Tuygun, M. (2019, Haziran). *ISO 27001 Bilgi Güvenliği Yönetim Sistemi Standardının Kamu Kurumlarına Uygulanabilirliğinin Araştırılması: Ankara İli Örneği*, Yüksek Lisans Tezi, Gazi Üniversitesi Bilişim Enstitüsü, Ankara.

Türk Standardları Enstitüsü. (2006). *Bilgi Teknolojisi–Güvenlik Teknikleri-Bilgi Güvenliği Yönetim Sistemleri-Gereksinimler*. Ankara: Türk Standardları Enstitüsü, 1.

Türk Standardları Enstitüsü. (2013). *TS ISO/IEC 27001 Bilgi Güvenliği Yönetim Sistemi Standardı*. Ankara: Türk Standardları Enstitüsü, 1.

Türk Standardları Enstitüsü. (2017). *TS ISO/IEC 27001 Bilgi Güvenliği Yönetim Sistemi Standardı*. Ankara: Türk Standardları Enstitüsü, 1.

Türkiye Bilimsel ve Teknolojik Araştırma Kurumu Bilişim ve Bilgi Güvenliği İleri Teknolojiler Araştırma Merkezi Siber Güvenlik Enstitüsü. (2013). *Kamu Kurumlarının Uyması Gereken Asgari Bilgi Güvenliği Kriterleri*. Ankara: Ulaştırma, Denizcilik ve Haberleşme Bakanlığı, 1.

Türkiye Bilimsel ve Teknolojik Araştırma Kurumu Bilişim ve Bilgi Güvenliği İleri Teknolojiler Araştırma Merkezi Yazılım Teknolojileri Araştırma Enstitüsü. (2017). *Dijital Olgunluk*. Ankara: Türkiye Bilimsel ve Teknolojik Araştırma Kurumu Bilişim ve Bilgi Güvenliği İleri Teknolojiler Araştırma Merkezi Yazılım Teknolojileri Araştırma Enstitüsü, 1.

Türkiye Bilimsel ve Teknolojik Araştırma Kurumu Bilişim ve Bilgi Güvenliği İleri Teknolojiler Araştırma Merkezi Siber Güvenlik Enstitüsü. (2017). *İşletim ve Bakım Rehberi. Dijital Olgunluk Modeli ve Rehberliği*. Kocaeli: Türkiye Bilimsel ve Teknolojik Araştırma Kurumu Bilişim ve Bilgi Güvenliği İleri Teknolojiler Araştırma Merkezi Siber Güvenlik Enstitüsü, 1.

Türkiye Bilimsel ve Teknolojik Araştırma Kurumu Bilişim ve Bilgi Güvenliği İleri Teknolojiler Araştırma Merkezi Siber Güvenlik Enstitüsü. (2021). *Bilgi Güvenliği ve Yönetimi Rehberi İşletim ve Bakım. Dijital Kabiliyet Rehberleri.* Kocaeli: Türkiye Bilimsel ve Teknolojik Araştırma Kurumu Bilişim ve Bilgi Güvenliği İleri Teknolojiler Araştırma Merkezi Siber Güvenlik Enstitüsü, 1.

Türkiye Odalar ve Borsalar Birliği. (2013). *Sorularla Örnekleme, Araştırma ve Veri Derleme*. Ankara: Türkiye Odalar ve Borsalar Birliği, 32.

Tvrdikova, M. (2008). *Information System Integrated Security.* 2008 7th Computer Information Systems and Industrial Management Applications. USA: IEEE, 153-154.

Ulaştırma, Denizcilik ve Haberleşme Bakanlığı. (2013). *Ulusal Siber Güvenlik Stratejisi ve 2013-2014 Eylem Planı*. Ankara: Ulaştırma, Denizcilik ve Haberleşme Bakanlığı, 1.

Ulaştırma, Denizcilik ve Haberleşme Bakanlığı. (2014). *Sektörel SOME Kurulum ve Yönetim Rehberi*. Ankara: Ulaştırma, Denizcilik ve Haberleşme Bakanlığı, 30.

Ulaştırma, Denizcilik ve Haberleşme Bakanlığı. (2015). *KamuNet Projesi.* Ankara: Ulaştırma, Denizcilik ve Haberleşme Bakanlığı, 1.

Ulaştırma, Denizcilik ve Haberleşme Bakanlığı. (2017, Haziran 21). *KamuNet Ağına Bağlanma ve KamuNet Ağının Denetimine İlişkin Usul ve Esaslar Hakkında Tebliğ*. Ankara: Ulaştırma, Denizcilik ve Haberleşme Bakanlığı, 1.

Vural, Y. (2007). *Kurumsal Bilgi Güvenliği ve Sızma (Penetrasyon) Testleri*, Yüksek Lisans Tezi, Gazi Üniversitesi Fen Bilimleri Enstitüsü, Ankara.

Vural, Y., ve Sağıroğlu, Ş. (2008). Kurumsal Bilgi Güvenliği ve Standartları Üzerine Bir İnceleme. *Gazi Üniversitesi Mühendislik Mimarlık Fakültesi Dergisi*, 507-522.

Woodhouse, S. (2007). *Information Security: End User Behavior and Corporate Culture.* Seventh International Conference on Computer and Information Technology. 767-774.

EKLER

EK-1. Anket formu

Kamu Kurumlarının Bilgi Güvenliği Politikalarının Kurumsal Bilgi Güvenliğinin Sağlanması Açısından Uygulanabilirliğinin ve Etkinliğinin Analiz Edilmesi Konulu Anket Çalışması

Değerli Katılımcılar,

Bu anket; Gazi Üniversitesi Fen Bilimleri Enstitüsü Bilgi Güvenliği Mühendisliği Ana Bilim Dalında gerçekleştirilen "Kamu Kurumlarının Bilgi Güvenliği Politikalarının Kurumsal Bilgi Güvenliğinin Sağlanması Açısından Uygulanabilirliğinin ve Etkinliğinin Analiz Edilmesi" konulu yüksek lisans tezinin bir parçasıdır. Anket, halihazırda bilgi güvenliği politikası olan kamu kurum ve kuruluşlarında görev yapan bilgi işlem/bilgi sistemleri birimi çalışanları veya bilgi teknolojileri/güvenliği projelerinde görev alan kişiler tarafından cevaplandırılacaktır. Elde edilecek veriler kişisel değerlendirmeye tabi tutulmayacak, sadece bilimsel amaçla kullanılacak olup, değerlendirmelerde kişi adı, kurum adı ya da kurum adını gösterecek tanımlamalara kesinlikle yer verilmeyecektir.

Araştırmanın bulguları bilimsel amaçlı olarak kullanılacağı için katılımcıların anketi doğru yanıtlamaları bu açıdan önemlidir. Anketin uygulanması için gerekli etik kurul izni alınmıştır. Anketin cevaplanma süresi ortalama 10 dakikadır.

Çalışmamıza katkılarınız için ve kıymetli zamanınızı ayırdığınız için teşekkür ederiz.

Samime MERAL

Gazi Üniversitesi, Fen Bilimleri Enstitüsü
Bilgi Güvenliği Mühendisliği Ana Bilim Dalı

Bu çalışmaya tamamen gönüllü olarak katılıyorum, istediğim zaman yarıda bırakıp çıkabileceğimi biliyorum ve verdiğim cevapların bilimsel amaçlı olarak kullanılmasını kabul ediyorum.

Onay Veriyorum [ ]

EK-1. (devam) Anket formu

BÖLÜM I - DEMOGRAFİK BİLGİLER

Lütfen her soru için size en uygun seçeneği işaretleyiniz.

1. **Cinsiyetiniz:** Kadın [ ] Erkek [ ]
2. **Yaşınız:** 18-20 [ ] 21-30 [ ] 31-40 [ ] 41-50 [ ] 50 yaş üstü [ ]
3. **Eğitim Düzeyiniz:** Lise ve altı [ ] Ön Lisans [ ] Lisans [ ] Yüksek Lisans [ ] Doktora [ ]
4. **Görev Yaptığınız Kurumda Çalışma Süreniz:** 1 yıl ve daha az [ ] 2-5 yıl [ ] 6-10 yıl [ ] 10-14 yıl [ ] 15 yıl ve üzeri [ ]
5. **Görev Yaptığınız Kurumda Çalışma Alanınız:**

   Birden fazla alanda çalışma durumunuz var ise lütfen sizi tanımlamaya en uygun alanı seçiniz.

   Yazılım Geliştirme [ ] Yazılım Kalite ve Test [ ] Mobil Uygulama Geliştirme [ ] Ağ ve Sistem Yönetimi [ ] Bilgi Güvenliği/Siber Güvenlik [ ] Veri Tabanı Yönetimi [ ] Bilgi İşlem Teknik Destek [ ] Bilgi Teknolojileri Denetimi [ ] Bilgi Teknolojileri Proje Yönetimi [ ] Diğer [ ]

EK-1. (devam) Anket formu

BÖLÜM II – KURUMSAL YAPIYA İLİŞKİN BİLGİLER

1. **Kurumunuzun Sahip Olduğu Verilerin Kritiklik Düzeyini Seçiniz:**

   Aşağıda, Cumhurbaşkanlığı Dijital Dönüşüm Ofisi Bilgi ve İletişim Güvenliği Rehberi'nde yer alan kritik altyapı tanımı bulunmaktadır. Kurumun sahip olduğu verilerin kritiklik düzeyine, söz konusu Rehberde belirtilen kritik altyapılara ait verilerin Kurumda barındırılma oranına göre karar verilebilir.

   > *"Kritik Altyapı: İşlediği bilgi/verinin gizliliği, bütünlüğü veya erişilebilirliği bozulduğunda can kaybına, büyük ölçekli ekonomik zarara, ulusal güvenlik açıklarına veya kamu düzeninin bozulmasına yol açabilecek bilişim sistemlerini barındıran altyapılardır."*

   Çok Düşük [ ] Düşük [ ] Orta [ ] Yüksek [ ] Çok Yüksek [ ]

2. **Kurumunuzun İş Süreçlerinde Bilgi Sistemlerinin Kullanılma Yoğunluğunu Seçiniz:**

   Çok Düşük [ ] Düşük [ ] Orta [ ] Yüksek [ ] Çok Yüksek [ ]

EK-1. (devam) Anket formu

BÖLÜM III - BİLGİ GÜVENLİĞİ POLİTİKALARININ ETKİNLİĞİ

Lütfen görev aldığınız kurumu göz önünde bulundurarak, her soru için size en uygun seçeneği işaretleyiniz.

No	Maddeler	Kesinlikle Katılıyorum	Katılıyorum	Ne Katılıyorum Ne Katılmıyorum	Katılmıyorum	Kesinlikle Katılmıyorum
1	Bilgi güvenliği politikası açık ve anlaşılır bir dilde yazılmıştır.					
2	Bilgi güvenliği politikası bilgi güvenliği gereksinimlerine uygun şekilde hareket etmem konusunda yeterince yol göstericidir.					
3	Bilgi güvenliği politikası tüm çalışanların erişebileceği bir alanda tutulmaktadır.					
4	Bilgi güvenliği politikası kapsamında diğer dokümanlar (politika, prosedür, form, iş süreci, talimat vb.) oluşturulmuştur.					
5	Bilgi güvenliğinin sağlanması konusunda koordinasyonu sağlayacak bir bilgi güvenliği koordinasyon kurulu/yönetimi vardır.					
6	Yönetim, bilgi sisteminin kurum amaçlarına uygun çalışmasını ve işlevlerini doğru bir şekilde yerine getirmesini sağlayacak tedbirleri almaktadır.					
7	Yürütülen çalışmalarda bilgi güvenliğinin sağlanması açısından görevler ayrılığı ilkesine uygun davranılmaktadır.					
8	İş süreçlerinde görevler ayrılığı ilkesinin uygulanabilmesi için yeterli sayıda ve nitelikte personel bulunmaktadır.					
9	Bilgi güvenliğinin sağlanması açısından az yetki ve bilmesi gereken prensibine uygun hareket edilmektedir.					
10	Bilgi güvenliği çalışmaları iyi bir şekilde yönetilmektedir.					
11	Gerçekleştirilen bilgi güvenliği farkındalık çalışmaları yeterli ve amacına uygundur.					

EK-1. (devam) Anket formu

12	Yönetim, bilgi teknolojileri alanında çalışan ve bilgi güvenliği organizasyonunda yer alan personelin güncel bilgi güvenliği konularından haberdar olması adına personel gelişimini destekleyici tutum ve davranışlar ortaya koymaktadır.					
13	Sahip olunan bilgi varlıklarına ilişkin envanter tutulmaktadır ve güncelliği sağlanmaktadır.					
14	Bilgi varlıklarının gizlilik değerlerine ilişkin bilgi sınıflandırması (gizli, çok gizli vb.) yapılmaktadır.					
15	Sahip olunan bilgi varlıklarına ilişkin etkin bir risk değerlendirme çalışması yapılmaktadır.					
16	Risklere karşı tanımlanan düzeltici ve iyileştirici faaliyetler yeterli seviyededir.					
17	Sistem, parolamı belirli uzunluk ve karmaşıklıkta oluşturmak için beni zorlamaktadır.					
18	Sistem, parolamı belirli aralıklarla değiştirmem için beni zorlamaktadır.					
19	Sistem, önceden kullandığım parolaları tekrar kullanmama izin vermemektedir.					
20	Sahip olduğum kullanıcı adı ve parola gibi bilgilerin gizliliği tarafımca yeterli bir şekilde sağlanmaktadır.					
21	E-posta güvenliğine ilişkin çözümler (spam koruması, zararlı bağlantılara erişimin engellenmesi vb.) uygulanmaktadır.					
22	Kurum ağına bağlı sahip olduğum cihazlarda antivirüs programı çalışmaktadır.					
23	Yetkisiz erişimler de dahil olmak üzere iç ağı, dış tehditlerden korumak için güvenlik önlemleri (güvenlik duvarı vb.) alınmaktadır.					
24	Kurumsal uygulamalara erişim sağlarken kimlik doğrulama mekanizması kullanılmaktadır.					
25	Kritik sistemlere erişimde çoklu kimlik/çok faktörlü doğrulama mekanizmaları (MFA, 2FA) kullanılmaktadır.					
26	Son kullanıcı aktiviteleri (log, denetim izi), güvenlik zafiyetleri ve bilgi sızdırmalarına karşı kayıt altına alınmaktadır.					
27	Kurum ağından güvenilir olmayan sitelere erişim kısıtlanmaktadır.					
28	Kurum ağına uzaktan erişim yalnızca güvenli uzaktan bağlantı sağlayan sistemler (VPN vb.) üzerinden gerçekleştirilmektedir.					

EK-1. (devam) Anket formu

29	Kurum ağının saldırılara karşı korunabilmesi için gerekli güvenlik çözümleri (IPS, IDS, DDoS, WAF vb.) kullanılmaktadır.					
30	Düzenli olarak sızma testi ve güvenlik denetimleri gerçekleştirilmektedir.					
31	Bağlantı yaptığım sistemde uzun süre aktif olmadığım durumda bağlantımın sona erdirilmesi için oturum zaman aşımı süresi çözümü uygulanmaktadır.					
32	Kurum bünyesinde geliştirilen uygulamalarda güvenli yazılım geliştirme yaşam döngüsü süreçleri ve modellerinden faydalanılmaktadır.					
33	Uygulama güvenliği için önlemler (sql injection, xss saldırılarının önlenmesine yönelik çalışmalar, insan robot davranışlarını birbirinden ayırt etmeye yarayan captcha çözümleri vb.) alınmaktadır.					
34	Bilgi güvenliğini etkileyen kurum iş süreçleri, bilgi işleme olanakları ve sistemlerdeki değişikliklere ilişkin planlama ve test çalışmaları yapılmaktadır.					
35	Yürütülen çalışmalarda geliştirme, test ve üretim ortamları mantıksal olarak birbirinden ayrılmıştır.					
36	Yürütülen çalışmalarda bilgi güvenliği gereksinimleri için etkin bir test süreci işletilmektedir.					
37	Olası felaket durumlarında veya iş akışını engelleyecek, aksatacak her türlü senaryonun gerçekleşmesi halinde, bilgi güvenliği sürekliliğinin sağlanması için gerekli önlemler alınmaktadır.					
38	Tedarikçiler ve üçüncü taraf çalışanları ile gizlilik anlaşmaları yapılmaktadır.					
39	Tedarikçiler tarafından sağlanan hizmetlerde bilgi güvenliği riskleri oluşturabilecek durumlara karşı dikkatli davranılmaktadır.					
40	Kurum binasında fiziksel güvenlik önlemleri alınmaktadır.					
41	Belirli kritik alanlara giriş ve çıkışlarda elektronik kapı, turnike, görüntü/ses kayıtları gibi fiziksel güvenlik önlemleri uygulanmaktadır.					
42	Bilgisayar monitörlerinde, çalışma masası üstlerinde, bilgisayar kasalarında güvenlik ihlaline neden olacak nitelikte parola, gizli bilgi, belge vb. bulundurulmaması konusunda özen gösterilmektedir.					

EK-1. (devam) Anket formu

43	Kritik bilgi barındıran ve yok edilmesi gereken ortamlar (belge, disk vb.) için imha kuralları işletilmektedir.					
44	İş ihtiyaçları için taşınabilir bellek kullanılması gerektiği durumlarda güvenlik tedbirleri (kurum tarafından yetkilendirilmiş ve kurum envanterine kaydedilmiş, parola ile erişim sağlanan taşınabilir bellek kullanılması vb.) uygulanmaktadır.					
45	Mobil cihazlar üzerine yazılım kurulumuna yönelik kısıtlamalar uygulanmaktadır.					
46	Sahip olduğum kişisel cihazım ile kurum ağına bağlanmam gerektiği durumda gerekli güvenlik tedbirleri uygulanmaktadır.					
47	Bilgi varlıklarının amacına uygun kullanılmadığı durumlarda yaşanması muhtemel bilgi güvenliği ihlal olaylarından dolayı devreye girebilecek bir disiplin süreci oluşturulmuştur.					
48	Bilgi güvenliği ihlal olaylarına zamanında ve uygun karşılık verilebilmektedir.					

EK-2. Etik komisyonu kararı

Evrak Tarih ve Sayısı: 24.06.2021-E.113099

T.C.
GAZİ ÜNİVERSİTESİ
Etik Komisyonu

Sayı : E-77082166-302.08.01-113099 24.06.2021
Konu : Bilimsel ve Eğitim Amaçlı

FEN BİLİMLERİ ENSTİTÜSÜ MÜDÜRLÜĞÜNE

Üniversitemiz Fen Bilimleri Enstitüsü Bilgi Güvenliği Mühendisliği Anabilim Dalı **Yüksek Lisans Öğrencisi Samime MERAL'in, Prof.Dr.Halil İbrahim BÜLBÜL'ün** danışmanlığında yürüttüğü *"Kamu Kurumlarının Bilgi Güvenliği Politikalarının Kurumsal Bilgi Güvenliğinin Sağlanması Açısından Uygulanabilirliğinin ve Etkinliğinin Analiz Edilmesi"* adlı tez çalışması ile ilgili konu Komisyonumuzun **22.06.2021** tarih ve **11** sayılı toplantısında görüşülmüş olup,

İlgilinin çalışmasının, yapılması planlanan yerlerden izin alınması koşuluyla yapılmasında etik açıdan bir sakınca bulunmadığına oybirliği ile karar verilmiş ve karara ilişkin imza listesi ekte gönderilmiştir.

Bilgilerinizi rica ederim.

Araştırma Kod No: 2021 - 674

Prof. Dr. İsmail KARAKAYA
Komisyon Başkanı

Ek:1 Liste
DAĞITIM
Gereği:
Sayın Prof. Dr. Halil İbrahim BÜLBÜL

Bilgi:
Fen Bilimleri Enstitüsü Müdürlüğüne

EK-2. (devam) Etik komisyonu kararı

GAZİ ÜNİVERSİTESİ
ETİK KOMİSYONU KATILIM LİSTESİ

TOPLANTI TARİHİ : 22.06.2021	TOPLANTI SAYISI : 11
ADI – SOYADI	**İMZA**
Prof. Dr. İsmail KARAKAYA BAŞKAN	
Prof.Dr.Kemal ÖZTEMEL BAŞKAN YRD.	
Prof.Dr.C.Haluk BODUR	
Prof.Dr.Seçil ÖZKAN	
Prof.Dr.Cevriye TEMEL GENCER	
Prof.Dr.İsmet YÜKSEL	
Prof.Dr.Aymelek GÖNENÇ	
Prof.Dr.Gülay BAYRAMOĞLU	
Prof.Dr.Makbule GEZMEN KARADAĞ	
Prof.Dr.Zehra GÖÇMEN BAYKARA	
Doç.Dr.İlyas OKUR	
Doç.Dr.Nihan KAFA	
Doç.Dr.Melek Gülşah ŞAHİN	

GAZİ GELECEKTİR...