GU J Sci, Part C, 10(2): 314-329 (2022)

Gazi Üniversitesi

Fen Bilimleri Dergisi

PART C: TASARIM VE TEKNOLOJİ

http://dergipark.gov.tr/gujsc

Analysis of the Efficiency of the Information Security Policies of Public Institutions in terms of Ensuring Corporate Information Security

Samime MERAL[1,*] Halil İbrahim BÜLBÜL[2]

[1]*Gazi Üniversitesi, Fen Bilimleri Enstitüsü, Bilgi Güvenliği Mühendisliği Anabilim Dalı, 06500, Yenimahalle/ANKARA*

[2]*Gazi Üniversitesi, Gazi Eğitim Fakültesi, Bilgisayar ve Öğretim Teknolojileri Bölümü, 06500, Yenimahalle/ANKARA*

Makale Bilgisi

Araştırma makalesi
Başvuru: 27.09.2021
Düzeltme: 09.10.2021
Kabul: 04.04.2022

Keywords

Information Security
Corporate Information Security
Information Security Policies
Information Security Management System

Anahtar Kelimeler

Bilgi Güvenliği
Kurumsal Bilgi Güvenliği
Bilgi Güvenliği Politikaları
Bilgi Güvenliği Yönetim Sistemi

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.

Kamu Kurumlarının Bilgi Güvenliği Politikalarının Kurumsal Bilgi Güvenliğinin Sağlanması Açısından Etkinliğinin Analiz Edilmesi

Öz

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

*Corresponding author, e-mail: samime.meral@gazi.edu.tr
DOI: 10.29109/gujsc.1001706

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.

1. GİRİŞ (INTRODUCTION)

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 [1]. 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 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.

Kurumlar bilgi güvenliğini sağlamaya yönelik yürütecekleri çalışmalara başlarken ilk olarak her türlü bilgi güvenliği faaliyetine 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. 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 [2]. Bilgi güvenliği politikasında, bilgi güvenliğinin sağlanabilmesi ve belirlenen hedeflerin amacına ulaşabilmesi için yapılması gerekenler ifade edilmektedir. 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 [3]. 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. Bu çalışmaların başında Uluslararası Standardizasyon Örgütü (ISO) 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 (UDHB) tarafından 2017 yılında KamuNet Ağına Bağlanma ve KamuNet Ağının Denetimine İlişkin Usul ve Esaslar Hakkında Tebliğ (Tebliğ) yayımlanmıştır. 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 'Kamu Kurumlarının Uyması Gereken Asgari Bilgi Güvenliği Kriterleri'" dokümanı hazırlanmıştır [8]. Bilgi güvenliği kriterlerinin yer aldığı dokümanda, tüm kurumlar tarafından bilgi güvenliği politika dokümanının yayınlanması gerektiği açıkça ifade edilmektedir.

Diğer önemli çalışma ise Cumhurbaşkanlığı Dijital Dönüşüm Ofisi (CB DDO) uhdesinde hazırlanan ve yayınlanan Bilgi ve İletişim Güvenliği Rehberi (Rehber)'dir. Söz konusu Rehber, 6 Temmuz 2019 tarihli Cumhurbaşkanlığı Bilgi ve İletişim Güvenliği Tedbirleri Genelgesi (Genelge) uyarınca hazırlanarak Temmuz 2020'de yayınlanmıştır [9]. Genelge'de tüm kurumların Rehber'e uygun hareket etmesi gerektiği vurgulanmıştır. Rehber'de [10] 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.

Bilgi güvenliği yalnızca bilgi sistemlerinin güvenliğini içermemektedir. Kurumsal bilgi güvenliği insan faktörü, eğitim, teknoloji gibi birçok faktörün etki ettiği tek bir çatı altında yönetilmesi zorunlu olan karmaşık süreçlerden oluşmaktadır. Bu nedenle bilginin iyi bir şekilde güvence altına alınması ve etkin bir şekilde yönetilmesi önemlidir [11]. Bilgi güvenliğine yönelik güvenlik risk ve açıklıkları bilgi sistemlerini yöneten kimselerden kaynaklanabileceği gibi sistemdeki yazılım, donanım, vb. unsurlardan da kaynaklanabilmektedir [12]. Bilgi sistemlerinin güvenliğinde donanım, yazılım, insan faktörü, veriler ve dış ortamın etkileri gibi tüm parçalarının güvenliği göz önünde bulundurulmalıdır [13]. 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 vb. ekseninde insan faktörlü etkiler üzerine odaklanıldığı görülmektedir. Özdemir [12] 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 [14] 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 [15] 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 [16] 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 [17] 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 [18] 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 [19] 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 [20] 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 [16] 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 [21] 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 [22] 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.

Çalışmanın ikinci bölümünde araştırma yöntemine, üçüncü bölümünde araştırma bulgularına ve son bölümünde araştırma sonuçlarına yer verilmiştir.

2. MATERYAL VE METOTLAR (MATERIALS AND METHODS)

Bu bölümde; araştırmanın amacı, önemi, modeli, evren ve örneklemi, kapsam ve sınırlılıkları, varsayımları, veri toplama aracı, çalışma grubu ve araştırma verilerinin analizine ilişkin yapılan istatistiki testler ele alınmıştır.

2.1. Araştırmanın Amacı ve Önemi (Objective and Importance of the Research)

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 edilmesi amaçlanmıştır.

Bu temel amaç doğrultusunda oluşturulan araştırma soruları aşağıda belirtilmiştir:

- Kamu kurumlarının bilgi güvenliği politikalarının etkinliği ile ilgili mevcut durum nedir?
- Kamu kurumlarının sahip olduğu verilerin kritiklik düzeyi ile bilgi güvenliği politikalarının etkinliği arasında istatistiksel açıdan anlamlı düzeyde bir farklılık bulunmakta mıdır?
- Kamu kurumlarının iş süreçlerinde bilgi sistemleri kullanılma yoğunluğu ile bilgi güvenliği politikalarının etkinliği arasında istatistiksel açıdan anlamlı düzeyde bir farklılık 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 kullanılma yoğunluğu için;

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

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.

2.2. Araştırmanın Modeli (Model of the Research)

Araştırmada yöntem olarak, olgu ve olayları nesnelleştirerek gözlemlenebilir, ölçülebilir ve sayısal olarak ifade edilebilir bir şekilde ortaya koymaya yarayan [23] 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 [24] betimsel tarama modeli kullanılmıştır. Bu kapsamda mevcut durumun analiz edilebilmesi için anket çalışması yapılmıştır.

2.3. Araştırma Evreni ve Örneklemi (Research Population and Sample)

"Elektronik Kamu Bilgi Yönetim Sistemi"nde (KAYSİS)[1] yer alan bakanlıklar ve bu bakanlıklar ile bağlı/ilgili/ilişkili kurumlar olmak üzere 17 kamu kurumu 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 [25]. 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 [26]. 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 [27]. Küme örnekleme yöntemiyle seçilen kurumlar, kritik altyapı sektörlerini düzenleyen ve bu kapsamda olmayan kurumlar olacak şekilde gruplara ayrılmıştır. CB DDO Rehber'de [10] 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 [7] kamu kurumlarını kritik bilgi sistemleri[2] barındıran kritik kamu kurumları ve barındırmayan kurumlar diğer kurumlar olmak üzere sınıflandırılmıştır. Sektörel SOME Kurulum ve Yönetim Rehberi (SOME Rehberi)'nde [28] kritik kamu hizmetleri[3] ifade edilmektedir. 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.

2.4. Araştırmadaki Varsayımlar (Assumptions in Research)

Araştırmada aşağıda belirtilen varsayımlar kabul edilmiştir:

- Araştırmaya katılan katılımcıların ankete verdikleri yanıtlar katılımcıların gerçek görüşlerini yansıtmaktadır.

---

[1] https://www.kaysis.gov.tr/

[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 [7].

[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, güvenlik (polis, jandarma, sahil güvenlik), yollar ve köprüler, barajlar, maaş ve adli işlemlerin yapıldığı ve kayıtlarının bulunduğu kritik sistemlerden sunulan servislerdir [28].

- Araştırmaya, örneklemi oluşturan kamu kurumlarının bilgi işlem/bilgi sistemleri birimi çalışanları ve/veya bilgi teknolojileri/güvenliği projelerinde görev alan çalışanlar katılmıştır.
- Örneklem alınan her bir kamu kurumu evreni yeterince temsil edebilecek durumdadır.

2.5. Araştırmanın Kapsamı ve Sınırlılıkları (Scope and Limitations of the Research)

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.

2.6. Veri Toplama Aracı (Data Collection Tool)

Araştırma verilerinin toplanması için anket tekniğinden yararlanılmıştır. Anket, bireylerin demografik özelliklerini ve tercihlerini belirlemek için ya da bir konu, durum, olay hakkında bilgi toplamaya yönelik çeşitli soruların bir araya getirilmesiyle oluşturulan veri toplama aracıdır [29]. Kamu kurumlarının bilgi güvenliği politikalarının kurumsal bilgi güvenliğinin sağlanması açısından etkinliğinin analiz edilebilmesi için 55 sorudan oluşan bir anket geliştirilmiştir. Ankette yer alan maddeler, istatistik alanında uzman 2 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 soruları; hali hazırda bilgi güvenliği politikası bulunan kurumların politikaları, CB DDO Rehber, Rehber'e ilişkin 2019 yılında yayınlanmış olan Genelge, ISO 27001 BGYS Standardı EK-A kontrol maddeleri ve TÜBİTAK BİLGEM Yazılım Teknolojileri Araştırma Enstitüsü (YTE) tarafından Ocak 2021'de yayınlanan Bilgi Güvenliği Yönetimi Rehberi[4] incelenerek hazırlanmıştır. Sorular belirlenirken, bilgi güvenliği politikalarında ortak olan ve kurumların yapısına göre değişmeyecek nitelikte olan hususlar baz alınmıştır. 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 sahip olduğu verilerin kritiklik düzeyi ve kurumun iş süreçlerinde bilgi sistemleri kullanılma yoğunluğu bilgilerinden 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, 17 alt ana başlıkta ele alınan 48 sorudan oluşmaktadır.

Anket Google Formlar web uygulaması aracılığıyla çevrimiçi olarak oluşturulmuştur.

2.7. Verilerin Analizi (Analysis of Data)

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 [31]. Likert tipi ölçümlerde ölçeğin iç tutarlılığını belirlemede Cronbach Alpha yöntemi kullanılır [32]. Bu yönteme göre aşağıdaki güvenilirlik düzeyi aşağıdaki şekilde belirlenir:

- $0{,}00 \leq \alpha \leq 0{,}40$ 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 Tablo 1'de verilmektedir.

[4] Detaylı bilgi için bkz."Bilgi Güvenliği Yönetimi Rehberi" [30].

Tablo 1. *Anket güvenirlik analizi*

Güvenirlik Katsayısı	
Cronbach's Alpha	Madde Sayısı
,960	48

Tablo 1'de görüldüğü üzere Cronbach Alpha (α) güvenirlik katsayısı anketin tümü için ,96 olarak hesaplanmıştır. Bu sebeple; anketin yüksek derecede güvenilir olduğu söylenebilir. Anketten elde edilen verilerin dağılım normalliğinin belirlenmesi amacıyla Kolmogorov-Smirnov ve Shapiro-Wilk normallik testleri uygulanmıştır. Anketten elde edilen verilere uygulanan basıklık (kurtosis) ve çarpıklık (skewness) katsayılarının -2, +2 arasında olduğu görülmüştür. Bu sebeple verilerin normal dağılım gösterdiği varsayılmıştır [33]. 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.

3. BULGULAR VE TARTIŞMA (FINDINGS AND DISCUSSION)

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.

3.1. Demografik Bilgiler (Demographic Information)

Ankete katılım sağlayan katılımcılara ait demografik özellikler Tablo 2'de verilmektedir.

Tablo 2*. Katılımcıların demografik özellikleri*

Bağımsız Değişken	**Grup**	**N = 121**	**Yüzde (%)**
Cinsiyet	Kadın	42	34,70
	Erkek	79	65,30
Yaş	21-30	31	25,60
	31-40	54	44,60
	41-50	27	22,30
	50 yaş üzeri	9	7,40
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
Görev Yapılan Kurumda 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
Görev Yapılan Kurumda 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

Tablo 2 incelendiğinde katılımcıların %34,70'i (N=42) kadın ve %65,30'u (N=79) erkektir. Araştırmaya katılan katılımcıların yaş gruplarına bakıldığında, %25,60'ı (N=31) 21-30 yaş grubunda, %44,60'ı (54) 31-40 yaş grubunda, %22,30'u (N=27) 41-50 yaş grubunda ve %7,40'ı (9) 50 yaş grubundadır. Tabloda 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. 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. 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.

3.2. Bilgi Güvenliği Politikalarının Etkinliğine İlişkin Bulgular (Findings Regarding the Effectiveness of Information Security Policies)

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. Katılımcıların bilgi güvenliği politikalarının etkinliği anketinden elde ettikleri katsayı ortalamaları Tablo 3'te verilmiştir.

Tablo 3. *Bilgi güvenliği politikalarının etkinliğine ilişkin bulgular*

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**

Tablo 3'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 tablodan; 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.

Tablo 3 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.

3.3. Bilgi Güvenliği Politikalarının Etkinliğinin Verilerin Kritiklik Düzeyine Göre Değişimine İlişkin Bulgular (Findings Regarding the Change in the Effectiveness of Information Security Policies According to the Criticality Level of the Data)

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 tek yönlü varyans analizi (ANOVA) tekniğinden yararlanılmıştır. Verilere söz konusu tekniğin uygulanması sonucu elde bulgular Tablo 4'te verilmiştir.

Tablo 4. *Bilgi güvenliği politikalarının etkinliğinin verilerin kritiklik düzeyine göre değişimine ilişkin bulgular*

	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			

Tablo 4'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.

Tablo 4'te 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.

Tablo 4'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 Tablo 5'te 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.

Tablo 5. *Kurumun sahip olduğu verilerin kritiklik düzeyi bağımsız değişkeninin gruplarının karşılaştırılması*

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

Tablo 5'e 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. Tabloda anlamlı farklılık olan gruplar * işareti ile ifade edilmiştir.

Tablo 5'te 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.

3.4. Bilgi Güvenliği Politikalarının Etkinliğinin Bilgi Sistemleri Kullanılma Yoğunluğuna Göre Değişimine İlişkin Bulgular (Findings Regarding the Change in the Effectiveness of Information Security Policies According to the Intensity of Using Information Systems)

Katılımcılar tarafından ankette yer alan sorulara verilen cevapların katsayı ortalamalarının, kamu kurumlarının iş süreçlerinde bilgi sistemleri kullanılma yoğunluğuna göre istatistiksel açıdan anlamlı düzeyde farklılık gösterip göstermediğinin belirlenmesi amacıyla tek yönlü varyans analizi (ANOVA) tekniğinden yararlanılmıştır. Verilere söz konusu tekniğin uygulanması sonucu elde bulgular Tablo 6'da verilmiştir.

Tablo 6. *Bilgi güvenliği politikalarının etkinliğinin bilgi sistemleri kullanılma yoğunluğuna göre değişimine ilişkin bulgular*

Kurumun İş Süreçlerinde Bilgi Sistemlerinin Kullanılma Yoğunluğu	**Grup**	**Frekans (f)**	**Ortalama**	**Oran (%)**	**Standart Sapma**
	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			

Tablo 6'da 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.

Tablo 6'da 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.

Tablo 6'da 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 Tablo 7'de verilmiştir.

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

Tablo 7. *Kurumun iş süreçlerinde bilgi sistemleri kullanılma yoğunluğu bağımsız değişkeninin gruplarının karşılaştırılması*

Kurumun İş Süreçlerinde Bilgi Sistemlerinin 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

Tablo 7'ye 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. Tabloda anlamlı farklılık olan gruplar * işareti ile ifade edilmiştir.

4. SONUÇ (CONCLUSION)

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 öğrenilmeye çalışılmıştır. Bu kapsamda çalışmada, kurumların sahip olduğu verilerin kritiklik düzeyi ve kurumların iş süreçlerinde bilgi sistemleri kullanılma 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.

Katılımcıların anketteki tüm sorulara verdiği cevaplar 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 değerlendirilmektedir.

Literatürdeki çalışmalarda [12, 14] 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.

Katılımcılar tarafından anketteki sorulara verilen cevaplar kurumun sahip olduğu verilerin kritiklik düzeyi bakımından değerlendirildiğinde; çok düşük, düşük, orta, yüksek ve çok yüksek grupları için bilgi güvenliği politikalarının etkinliğinin 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 değerlendirilmektedir. Benzer şekilde düşük ile çok yüksek grupları arasındaki farklılık düzeyinin de orta ile çok yüksek grupları arasındaki farklılık düzeyinden daha anlamlı olduğu değerlendirilmektedir.

Katılımcılar tarafından anketteki sorulara verilen cevaplar kurumun iş süreçlerinde bilgi sistemlerinin kullanılma yoğunluğu bakımından değerlendirildiğinde; çok düşük, düşük, orta, yüksek ve çok yüksek grupları için bilgi güvenliği politikalarının etkinliğinin 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 olduğu belirlenmiştir. Diğer grup eşleştirmeleri için p<0,05 şartı sağlanmadığı için anlamlı farklılık bulunmamaktadır.

Literatürde yer alan benzer çalışmalarda [12, 14, 15, 16, 17, 18, 19, 20] 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.

Araştırmada uygulanan anketin, araştırma konusunda teknik ve mesleki bilgiye sahip katılımcılar üzerinde gerçekleştirilmesinin, daha anlamlı sonuçların elde edilmesine katkı sağladığı değerlendirilmektedir.

Kurumların bilgi güvenliği politikalarının etkinlik değerlendirmeleri sonuçlarına göre kamu kurumlarına, etkinlik konusunda yetersiz olduğu ortaya konulan bilgi güvenliği konularının etkinliğinin sağlanması için ilave çalışmalar yapmaları önerilmektedir.

TEŞEKKÜR (ACKNOWLEDGMENTS)

Zaman ayırıp araştırma anketini doldurdukları için değerli katılımcılara teşekkür ederiz.

KAYNAKLAR (REFERENCES)

[1] Unescap. (2008). Information Security for Economic and Social Development.

[2] Kalman, S. (2003). Web Security Field Guide. Cisco Press, 36-37.

[3] Bhaharin, S. H., Mokhtar, U. A., Sulaiman, R., & Yusof, M. M. (2019). Issues and Trends in Information Security Policy Compliance. 2019 6th International Conference on Research and Innovation in Information Systems (ICRIIS).

[4] TSE. (2013). TS ISO/IEC 27001 Bilgi Güvenliği Yönetim Sistemi Standardı. Ankara: Türk Standardları Enstitüsü.

[5] T.C. Resmi Gazete. (2016, Aralık 3). Kamu Kurum ve Kuruluşlarının KamuNet'e Dahil Edilmesi ile İlgili 10016/28 Sayılı Başbakanlık Genelgesi. (29907).

[6] UDHB. (2013). 2013-2014 Ulusal Siber Güvenlik Stratejisi ve Eylem Planı. Ankara: T.C. Ulaştırma Denizcilik ve Haberleşme Bakanlığı.

[7] TÜBİTAK BİLGEM SGE. (2013). Kamu Kurumlarının Uyması Gereken Asgari Bilgi Güvenliği Kriterleri. Ankara: UDHB.

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

[9] T.C. Resmi Gazete. (2019, Temmuz 6). Bilgi ve İletişim Güvenliği Tedbirleri Genelgesi. (30823).

[10] Dijital Dönüşüm Ofisi. (2020, Temmuz). Bilgi ve İletişim Güvenliği Rehberi. Ankara, Türkiye: T.C. Cumhurbaşkanlığı.

[11] Thakur, K., Ali, M., Gai, K., & 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).

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

[13] Tvrdikova, M. (2008). Information System Integrated Security. 2008 7th Computer Information Systems and Industrial Management Applications.

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

[15] Solmaz, M. (2020, Nisan). Öğretmen Adaylarının Siber Bilgi Güvenliği Farkındalıklarının Ve Dijital Vatandaşlık Düzeylerinin Farklı Değişkenler Açısından İncelenmesi. Mersin: Mersin Üniversitesi Eğitim Bilimleri Enstitüsü Bilgisayar Ve Öğretim Teknolojileri Eğitimi Anabilim Dalı.

[16] Tuygun, M. (2019, Haziran). Iso27001 Bilgi Güvenliği Yönetim Sistemi Standardının Kamu Kurumlarına Uygulanabilirliğinin Araştırılması: Ankara İli Örneği. Yüksek Lisans Tezi. Ankara, Türkiye: Gazi Üniversitesi Bilişim Enstitüsü.

[17] Henkoğlu, T. (2015). Hassas Bilgi Varlıklarının ve Kişisel Verilerin Hukuksal Düzenlemeler ile Korunması ve Bu Kapsamda Üniversiteler İçin Bilgi Güvenliği Politikasının Geliştirilmesi. Ankara: T.C. Hacettepe Üniversitesi Sosyal Bilimler Enstitüsü Bilgi ve Belge Yönetimi Anabilim Dalı.

[18] Çek, E. (2017). Kurumsal Bilgi Güvenliği Yönetişimi ve Bilgi Güvenliği için İnsan Faktörünün Önemi. İstanbul Bilgi Üniversitesi Sosyal Bilimler Enstitüsü Bilişim ve Teknoloji Hukuku Yüksek Lisans Programı.

[19] Şişkin, D. Ş. (2020). Üniversite Kütüphanelerinde Bilgi Güvenliği ve Kişisel Verilerin Korunması: Ankara'daki Üniversite Kütüphanelerinin Değerlendirilmesi. Ankara: Hacettepe Üniversitesi Sosyal Bilimler Enstitüsü Bilgi ve Belge Yönetimi Anabilim Dalı.

[20] Vural, Y. (2007, Mayıs). Kurumsal Bilgi Güvenliği Ve Sızma (Penetrasyon) Testleri. Ankara: Gazi Üniversitesi Fen Bilimleri Enstitüsü.

[21] Özcan, B. (2009). Kurumsal Bilgi Güvenliği ve Cobit. T.C. Haliç Üniversitesi Fen Bilimleri Enstitüsü Yönetim Bilişim Sistemleri AnaBilim Dalı.

[22] Çetinkaya, M. (2008, Eylül). Bilgi Güvenliği Yönetim Sistemi Alt Yapısının Değerlendirilmesi İçin Bir Test Aracı Geliştirilmesi. T.C. İstanbul Kültür Üniversitesi Fen Bilimleri Enstitüsü Bilgisayar Mühendisliği Ana Bilim Dalı.

[23] Gurbetoğlu, A. (2018). Bilimsel Araştırma Yöntemleri. İstanbul: İstanbul Sabahattin Zaim Üniversitesi Eğitim Fakültesi.

[24] Karasar, N. (1999). Bilimsel Araştırma Yöntemi. Ankara: Nobel Yayın Dağıtım.

[25] İftar, G. K. (1999). Bilim ve Araştırma. K. Özdamar, Y. Odabaşı, Y. Hoşcan, A. A. Bir, G. Kırcaali İftar, A. Özmen, & Y. Uzuner içinde, Sosyal Bilimlerde Araştırma Yöntemleri. Eskişehir: T.C. Anadolu Üniversitesi Açıköğretim Fakültesi.

[26] T.C. Ankara Üniversitesi. (2012, Şubat 26). Evren, Örneklem, Örnekleme Türleri. Ağustos 30, 2021 tarihinde Ankara Üniversitesi Açık Ders Malzemeleri: https://acikders.ankara.edu.tr adresinden alındı

[27] Earl, J. (2004). Controlling protest: New directions for research on the social control of protest. Research in Social Movements, Conflicts and Change, 55-83.

[28] UDHB Haberleşme Genel Müdürlüğü. (2014, Kasım). Sektörel SOME Kurulum ve Yönetim Rehberi. Ankara: UDHB.

[29] Metin, M. (2014). Kuramdan Uygulamaya Eğitimde Bilimsel Araştırma Yöntemleri. Ankara: Pegem Akademi.

[30] TÜBİTAK BİLGEM YTE. (2021, Ocak). Bilgi Güvenliği ve Yönetimi Rehberi İşletim ve Bakım. Dijital Kabiliyet Rehberleri. Ankara.

[31] İslamoğlu, A., & Alnıaçık, Ü. (2016). Sosyal Bilimlerde Araştırma Yöntemleri. İstanbul: Beta Yayınları.

[32] Kılıç, B. (2019, Aralık). ISO/IEC 27001 Bilgi Güvenliği Yönetim Sistemi Açısından Türkiye'de Hukuk Bürolarında Bilgi Güvenliği Yönetimi. Gazi Üniversitesi Bilişim Enstitüsü Adli Bilişim Ana Bilim Dalı.

[33] Mallery, P., & George, D. (2010). 2010 SPSS for Windows Step by Step: A Simple Guide and Reference 17.0 update. Boston: Allyn & Bacon, c2010.