Üniversite Kütüphanelerinde Teknolojik ve Kurumsal Bilgi Güvenliği Önlemlerinin Uygulanma Yeterliliği*

Ali Kavak** Hüseyin Odabaş***

Öz

Amaç: *Bilgi güvenliği konusu, içinde bulunduğumuz dijital çağda üzerinde durulan önemli konulardan biridir. Özellikle de bilginin merkezi kütüphaneler için bu konu daha da önemli bir yerde durmaktadır. Diğer kütüphane türlerine kıyasla akademiysen ve öğrencilerin akademik çalışmaları ve eğitimleri için gerekli olan kaynakları ve hizmetleri sağlama konusunda özgünlükleriyle öne çıkan üniversite kütüphaneleri, bünyelerindeki bilgi varlıklarında kurumsal ve kişisel birçok veri ve bilgiyi barındırmaktadır. Bu nedenle bilgi güvenliği tüm kütüphane türlerinde olduğu gibi üniversite kütüphanelerinde de önemlidir. Ancak üniversite kütüphanelerinin bilgi ve kullanımı ile olan kendine özgü bağı, bu öneme farklı bir derinlik kazandırmaktadır. Bu çalışmada üniversite kütüphanelerinde bilgi güvenliği tehditlerine karşı teknolojik ve kurumsal bilgi güvenliği önlemlerinin uygulanma düzeylerinin tespiti ve yeterlilik durumlarının incelenmesi amaçlanmıştır.*

Yöntem: *Araştırmada, nicel araştırma yöntemlerinden tarama yöntemi kullanılmıştır. Araştırmanın evrenini Türkiye'de faaliyet gösteren üniversite kütüphanelerinde görev yapan personel oluşturmaktadır. Amaçlı örnekleme yöntemi ile bu evren içerisinde belirlenen örneklem gruba araştırma kapsamında geliştirilen anket uygulanmıştır.*

Bulgular: *Ankete verilen yanıtların analizinde, Türkiye'de üniversite kütüphanelerinde teknolojik ve kurumsal bilgi güvenliği önlemlerinin çoğunun "iyi" düzeyde uygulandığına ilişkin katılımcı görüşlerinin yüksek oranlarda olduğu görülmüştür. Bununla birlikte, söz konusu önlemlerin "hiç uygulanmadığı" veya "kötü" ve "orta" düzeylerde uygulandığı konusunda katılımcı görüşleri oranlarının da kayda değer düzeylerde olduğu belirlenmiştir.*

Sonuç: *Türkiye'deki üniversite kütüphanelerinde teknolojik ve kurumsal bilgi güvenliği önlemlerinin genel olarak orta düzeyin üzerinde uygulandığı, ancak bilgi güvenliği yönetimi açısından yeterli düzeylerde olmadığı sonucuna varılmıştır. Özellikle kurumsal bilgi güvenliği önlemlerin uygulanması konusundaki yeterliliğin daha düşük düzeylerde olduğu gözlemlenmiştir. Bu durumu etkileyen başlıca faktörler arasında, kurumsal farkındalık ve eğitim çalışmalarının eksikliği bulunmaktadır.*

Özgünlük: *Türkiye'de kütüphanecilik alanında bilgi güvenliği konusunda çalışmaların kısıtlı olması, özellikle üniversite kütüphaneleri özelinde bu konuda kapsamlı bir çalışmanın bulunmaması, bu çalışmayı özgün kılmaktadır. Ayrıca bilgi ve belge yönetimi disiplini*

* Bu makale 2023 yılında Çankırı Karatekin Üniversitesi Sosyal Bilimler Enstitüsünde hazırlanan "Üniversite Kütüphanelerinde Bilgi Güvenliği Yönetimi ve Bir Rehber Önerisi " başlıklı doktora tezinden türetilmiştir.

** Öğr. Gör. Dr., Samsun Üniversitesi, Kütüphane ve Dokümantasyon Daire Başkanlığı, a.kavak55@gmail.com

*** Prof. Dr., Çankırı Karatekin Üniversitesi, Bilgi ve Belge Yönetimi Bölümü, odabashuseyin@gmail.com

Geliş tarihi : 2 Temmuz 2023 *Kabul Tarihi: 18 Eylül 2023*
Makale Türü : Araştırma Makalesi

içerisinde yer alan tüm paydaşlarda bu konudaki farkındalığın gelişmesine katkı sunacağı düşünülen bu çalışma, gelecekte alana sunacağı yararlar bakımından nitelikli bir çalışma olarak değerlendirilmektedir.

Anahtar Sözcükler: *Üniversite kütüphaneleri, bilgi güvenliği, yönetim, kurumsal ve teknolojik önlemler.*

Adequacy of Implementation of Technological and Corporate Information Security Measures in University Libraries*

Ali KAVAK** Hüseyin Odabaş***

Abstract

Purpose: *Information security is one of the important topics emphasized in the digital age we are currently in. Particularly for central libraries, information security holds an even more significant place. University libraries, which stand out with their uniqueness in providing resources and services essential for academic research and education, house a multitude of institutional and personal data and information within their information assets. Therefore, information security is crucial in university libraries, as it is in other types of libraries. However, the distinct relationship that university libraries have with information and its usage adds a different depth to this importance. This study aims to determine the level of implementation and adequacy of technological and institutional information security measures against threats in university libraries.*

Method: *The study employs a quantitative research method, specifically the survey method. The population of the study consists of personnel working in university libraries in Turkey. A purposive sampling method was used, and a questionnaire developed for the research was administered to the selected sample group within this population.*

Findings: *In the analysis of the survey responses, it was observed that participant opinions regarding the implementation of technological and institutional information security measures in university libraries in Turkey were largely perceived as "good". However, noteworthy proportions of participant opinions indicated that these measures were either "not implemented at all" or implemented at "poor" and "moderate" levels.*

Implications: *It has been concluded that technological and corporate information security measures in university libraries in Turkey are generally implemented above the average level, but they are not at sufficient levels in terms of information security management. Particularly, the adequacy of corporate information security measures is observed to be at lower levels. One of the main factors influencing this situation is the lack of corporate awareness and training efforts.*

Originality: *The limited research on information security in the field of librarianship in Turkey, particularly the absence of comprehensive studies specifically focused on this subject in university libraries, makes this study unique. Furthermore, this study, which is believed to contribute to the awareness of all stakeholders within the discipline of information and*

* This article was produced from the doctoral thesis titled "Information Security Management in University Libraries and a Guide Proposal" prepared at Çankırı Karatekin University Social Sciences Institute in 2023.

** Lecturer. Dr., Samsun Üniversitesi, Library and Documentation Department, a.kavak55@gmail.com

*** Prof., Çankırı Karatekin University, Department of Information Management, odabashuseyin@gmail.com

Received : July 2,2023 Accepted: September 18, 2023
Type : Research Article

document management, is considered a valuable work in terms of its potential benefits to the field in the future.

Keywords: *University libraries, information security, management, corporate and technological measures.*

Giriş

Güvenlik, "toplum yaşamında yasal düzenin aksamadan yürütülmesi, kişilerin korkusuzca yaşayabilmesi durumu, emniyet" (Güvenlik, t.y.) olarak tanımlanmaktadır. Bu kavram, bir varlığın tehlikelerden uzak olma niteliğini ve durumunu kapsamaktadır. Diğer bir ifadeyle güvenlik, bir nesneyi ya da varlığı kasıtlı veya kasıtsız her türlü tehlikeden korumayı amaçlamaktadır. Güvenliğe duyulan ihtiyaç varlığın içinde bulunduğu faaliyet alanına ve büyüklüğüne göre şekillenmektedir. Örneğin devletler halkını, kaynaklarını ve diğer varlıklarını korumak için çok katmanlı ulusal bir güvenlik sistemine ihtiyaç duyarken, kurum veya kuruluşlar ise varlıklarını zararlı unsurlardan korumak için farklı güvenlik işlevlerine sahip güvenlik sistemlerine ihtiyaç duyabilmektedirler. Bu noktada çevresel ve fiziksel güvenlik, kurumsal güvenlik, iletişim ve haberleşme güvenliği, personel güvenliği, ağ güvenliği ve bilgi güvenliği gibi birçok farklı güvenlik sisteminin işler duruma getirilmesi kurumun sürekliliği açısından önemli görülmektedir (Whitman ve Mattord, 2011).

Bilgi, insanın çevresindeki nesneleri ve varlıkları yorumlaması, açıklaması veya yargılaması sonucu oluşan bir üründür. İnsan ile nesne arasında kurulan ilişkiden doğan bilgi, insanlık tarihinin en önemli sermayesi olarak görülmektedir. Bu sermayeyi gelecek kuşaklara sağlıklı biçimde aktarırken mahremiyetlerini korumak kurumsal ve kişisel bağlamda insanlık adına sorumluluk isteyen önemli bir ihtiyaçtır. Bu nedenle veri ve bilgilerin gizlilik, bütünlük ve erişilebilirlik unsurları çerçevesinde korunması önemlidir. Geçmişte bilginin güvenliğine yönelik birtakım önlemler geliştirildiği görülse de günümüzde bu konu üzerinde daha çok durulmaktadır. Gelişmiş ve gelişmekte olan toplumların son yıllarda toplumsal ve kurumsal yapılarında bilgi güvenliğine yönelik çalışmalara daha da önem verdiği anlaşılmaktadır. Teknolojik gelişmelere bağlı olarak kişisel ve kurumsal bilgilerin güvenliğine yönelik artan açıklar kontrol edilemez hale gelmiştir. Bu durum, bilgi güvenliğine yönelik çalışmaların artmasını sağlamıştır. Özellikle bilgi güvenliği yönetim sistemlerine yönelik çalışmalar kurum ve kişilerin üzerinde önemle durdukları bir süreç haline gelmiştir (Kemiksiz, 2022; Kara, 2018; Gülseçen, 2012).

Bilgisayar ve ağ teknolojilerindeki gelişmeler, bilginin üretildiği, korunduğu ve iletildiği ortamları da değişikliğe uğratmıştır (Polat, 2006). Özellikle son yıllarda elektronik ortamlar, bilginin en çok işlendiği ortamlar olmuştur. Bu gelişmeler, bilginin coğrafi ve fiziksel sınırlarını kaldırarak bilgiyi zaman ve mekândan bağımsız bir değer haline getirmiştir. Bilgi, gün geçtikçe artan değeriyle, devletlerin, kurumların ve bireylerin sahip olmak istediği önemli bir varlık durumuna gelmiştir. Bireylerin, bilgiyi güç unsuru olarak tanımlayarak değerlendirmesi ve ona sahip olma arzusu da bu süreçte daha da öne çıkmaktadır. Bilginin gücüne inanan ve bu gücü kullanmak

isteyen kişi ve kurumlar, bilişim ve iletişim teknolojilerine hızlı bir biçimde uyum sağlayarak bu araçları, hizmetlerine daha ileri düzeylerde değer katmak için kullanmaya başlamıştır. Bunula birlikte bu gücün güvenliğini sağlamanın bir gereksinim olduğunu görenler bu gücü güvenilir kılma arayışı içine de girmiştir. Bilişim teknolojileri ile doğrudan temas halinde olan sektörler ve bu sektörlere paydaş disiplinler bilgi güvenliği çalışmaları ve uygulamaları konusunda önemli mesafeler almıştır. Bu nedenle bilgisayar ve ağ teknolojileri, bilgi güvenliği çalışmalarının temel yapı taşlarını oluşturmuştur (Evrin ve Demirer, 2011).

Bilgi güvenliği, en genel ifade ile bilginin izinsiz veya yetkisiz bir biçimde erişiminin, kullanımının, değiştirilmesinin, ifşa edilmesinin, ortadan kaldırılmasının ve hasar verilmesinin önlenmesi olarak tanımlanmaktadır. Gizlilik, bütünlük ve erişilebilirlik, bilgi güvenliğinin vazgeçilmez üç temel unsurunu oluşturmaktadır. Bu üç temel güvenlik unsurundan herhangi birinin zarar görmesi bilgi güvenliği zafiyetinin varlığına işaret eder (Güngör, 2015; Marttin ve Pehlivan, 2010; Slade, 2006).

Whitman ve Mattord (2018), bilgi güvenliğinin bir kurumda dört ana görevi üstlendiğini belirtmektedir. Bunları; kurumun faaliyetlerini yürütebilme yeteneğinin korunması, kurumun bilgi sistemlerinde çalışan uygulamalarının performanslarının sağlanması, kurumun teknoloji varlıklarının korunması ve bu varlıklarda üretilen, işlenen ve depolanan verilerin korunması olarak özetlemektedir.

Bilgi güvenliği, bütün kurumlarda olduğu gibi kütüphanelerde ve diğer bilgi merkezlerinde de önemli bir konudur. Bilgi, kütüphane hizmetlerinin temelini oluşturan en önemli varlıktır; güvenliğine önemi nispetince değer verilmeli, güvenilir yöntemler ile yönetilmelidir. Kütüphanelerde bilgi güvenliğinin başarısı yöneticilerin, personelin, kullanıcıların ve diğer paydaşların nitelikli bilgi güvenliği farkındalığına ve bilincine sahip olmalarından geçmektedir. Bu başarıda en önemli rol hiç şüphesiz yöneticilere düşmektedir. Bilgi güvenliğinin ihmal edilmesi, kütüphane hizmetlerinin aksamasına ve telafi edilmesi uzun zaman alabilecek olumsuz sonuçlara yol açabilmektedir. Özellikle teknolojik araçların kütüphane hizmetlerinde daha yaygın olarak kullanılması, bilgi güvenliği yönetimine olan ihtiyacı daha da artırmaktadır (Pathari ve Sonar, 2012).

Bilişim ve iletişim teknolojilerinin hızlı gelişimi, kütüphanelerde kullanılan teknolojik araçların sayısını artırmış ve bu durum kütüphanelerin sahip olduğu bilgi varlıklarına ve bu varlıklar üzerinde kayıtlı veri ve bilgilere yönelik daha fazla güvenlik tehdidi üretmiştir. Bu nedenle bilgi varlıklarına işlenen bilgilerin korunması ve kullanıcılara güvenli bir biçimde iletilmesi giderek zorlaşmaktadır. Kullanıcıların ihtiyaç duyduğu bilgileri karşılamada önemli rol oynayan kütüphaneler, kullandığı ve kullanacağı yeni teknolojik

araçlara bağlı olarak hizmetlerinde ve kurumsal yapısında sürekli olarak değişim yaşamaktadır. Bu değişim kütüphanelerin bilgi güvenliği anlayışını da değişime mecbur kılmıştır. Teknolojik bilgi sistemlerinin yoğun bir biçimde kullanılmaya başlanması ile dijital bilgi güvenliği, kütüphaneler için öncelikli çalışma alanlarından biri olmuştur. Özellikle kütüphanelerde kullanılmaya başlayan çevrimiçi bilgi sistemleri ile sunulan hizmetlerin daha çok tercih edilmesiyle birlikte birçok güvenlik riski de yaşanmaya başlamıştır. Yüksek maliyetler ile satın alınan bilgi kaynaklarının yanı sıra kurumsal ve kişisel birçok önemli verinin depolandığı bilgi sistemleri, olası tehditlere ve saldırılara maruz kalmaktadır (Da Veiga ve Eloff, 2010; Gillaspy, 2005). Bu tehdit ve saldırıların en az kayıp ile giderilebilmesi için iyi bir kurumsal bilgi güvenliği yönetim sisteminin geliştirilmesi, uygulanması, değerlendirilmesi ve sürekli olarak iyileştirilmesi gerekmektedir.

Kütüphanelerde bilgi güvenliğine yönelik tehditlerin genellikle kurumsal bilgi güvenliği yönetimindeki bilgisizlik ve eksikliklerden kaynaklandığı bilinmektedir. Hizmetlerinin çoğunu bilgi sistemleri aracılığıyla yürüten kütüphanelerin bilgi varlıklarına karşı olası saldırılardan korunması amacıyla bilgi güvenliği ile ilgili gelişmeleri sürekli takip etmeleri, kütüphane yöneticilerine ve personeline yönelik bilgi güvenliği farkındalığı ve becerilerini geliştirici çalışmaları yürütmeleri, ulusal ve uluslararası standartlara uygun bir bilgi güvenliği yönetim sistemini geliştirmeleri gerekmektedir. Kurumsal bilgi güvenliği yönetimi ile güçlü bir bilgi güvenliği kültürü oluşturulur. Bu nedenle kütüphanelerde yöneticilerin tüm personeli ile birlikte kurumsal bilgi güvenliği yönetimi üzerinde önemle durması gerekir (Amini ve diğerleri, 2021; Peltier, 2016; Ismail, 2012; Thomson ve diğerleri, 2006; Workman ve diğerleri, 2008)

Gelişmiş ülkelerde kurumsal bilgi güvenliği ile ilgili araştırmaların Türkiye'ye göre daha erken dönemlerde yapılmaya başladığı ve Türkiye'de bu konunun daha çok kişisel bilgi güvenliği ile birlikte popülerlik kazandığı görülmektedir. Bu nedenle Türkiye'de kurumsal bilgi güvenliği yönetimi ile ilgili çok sayıda araştırma bulunmamakla birlikte, tamamlanan araştırmaların daha çok sağlık, bilişim, hukuk, finans ve iletişim gibi belirli hizmet sektörlerinde yoğunlaştığı görülmektedir (Çimen, 2021; Filik, 2020; Gürsel, 2019; H. Ö. Kurt, 2019; S. G. Kurt, 2019; Başdinkçi, 2017; Erol, 2016; Aksu, 2014; Şahinaslan, 2010). Kütüphaneler ve diğer bilgi merkezlerinde kurumsal bilgi güvenliği yönetimine ilişkin araştırmaların ise daha az sayıda olduğu anlaşılmaktadır (Şişkin, 2020; Henkoğlu ve Uçak, 2015; Öztemiz ve Yılmaz, 2013).

Dünya genelinde, kütüphanelerin hizmetleri açısından bilgi güvenliğinin hayati bir rol oynadığı birçok otorite (International Federation of Library Associations - IFLA, Association of College and Research Libraries - ACRL, American Library Association - ALA, International Organization for

Standardization – ISO, National Institute of Standards and Technology - NIST, Information Systems Audit and Control Association - ISACA vb.) tarafından kabul edilmektedir. Ancak kütüphanecilik alanında yapılan bilgi güvenliği çalışmalarının diğer hizmet alanlarına (sağlık, bankacılık, sigorta, iletişim) göre nispeten daha az ve yüzeysel olduğu gözlemlenmektedir. Bu duruma rağmen, son yıllarda bu alanda bazı gelişmeler yaşandığı görülmektedir. Bu çalışmanın, üniversite kütüphanelerinin bilgi sistemlerinde veya fiziksel ortamlarında işlenen bilgi ve verilerin gizlilik, bütünlük ve kullanılabilirlik ölçütleri bakımından ne düzeyde korunduğunun tespit edilmesi ve hangi bilgi güvenliği yöntemlerinin uygulanması gerektiği konusunda önerilerde bulunması açılarından alan yazına katkı sağlayacağı değerlendirilmektedir. Çalışmada üniversite kütüphanelerindeki bilgi güvenliği yönetiminin güçlü ve zayıf yönleri belirlenerek bu kurumlarda daha verimli ve güvenli bilgi hizmetlerinin yürütülebilmesi için bilgi güvenliği yönetiminde önceliklerin neler olması gerektiği, ne tür bilgi güvenliği mekanizmalarının geliştirilmesi ve hangi uygulamaların işler haline getirilmesi gerektiği ortaya konulmaktadır

Kütüphanelerde Bilgi Güvenliğinin Önemi

Kuşkusuz, günümüzün en değerli varlığı bilgidir. Bilgi çağı olarak adlandırılan bu çağın toplumuna ise bilgi toplumu denmektedir. Üniversiteler ise bu toplum yapısının gelişmesinde önderlik yapan kurumların başında gelmektedir. Bilgininin ekonomik, kültürel, sosyal ve sanatsal bir değer olarak işlendiği bu kurumlar, içinde bulunduğu toplumun bilgi seviyesine katkı sağlamaktadır. Bu nedenle bilgi ve bilgi varlıkları üniversitelerin dolayısıyla da kütüphanelerin temel hazinesini oluşturmaktadır.

Uluslararası Kütüphane Dernekleri ve Kurumları Federasyonunun yayımladığı kütüphane ortamının gizliliği bildirisinde (IFLA Statement on Privacy in the Library Environment), teknolojideki hızlı ilerlemelerin kütüphanelerin bilgi hizmetlerini ve dolayısıyla kullanıcılarının mahremiyetini etkilediği vurgulanmaktadır. Kütüphaneler, hizmetlerinde kullandığı bilgi varlıklarında çeşitli bilgi ve veriler barındırmaktadır. Bu bilgi ve verilerin içerisinde kurumsal bilgilerin yanı sıra personel, kullanıcı ve hatta diğer paydaşların bilgi ve verileri de yer almaktadır. Bu bilgi ve veriler gerek istatistik verilerin elde edilmesi için gerekse ticari amaçlar için hem kütüphaneler tarafından hem de kütüphanelerin ilişki içerisinde olduğu ticari kurumlar tarafından kullanılabilmektedir. Ayrıca bilgi sistemlerine yapılan saldırılar veya fiziksel girişimler ile bu bilgi ve veriler ifşa edilebilmektedir. Bu itibarla IFLA, İnsan Hakları Evrensel Beyannamesine de dayanarak yayımladığı bu beyannamede, bilgiye erişim ve ifade özgürlüğünün kütüphane ve bilgi mesleği için temel kavramlar olduğunu ve gizliliğin ise bu hakları sağlamanın ayrılmaz bir parçası olduğunu belirtmektedir. IFLA, kütüphanelerde gizliliğin sağlanması için yayımladığı bu beyannamede şu

önerileri sunmaktadır (International Federation of Library Associations [IFLA], 2015):

- Kütüphane ve bilgi hizmetleri, mahremiyete hem uygulama düzeyinde hem de ilke olarak saygı göstermeli ve geliştirmelidir.
- Kütüphane ve bilgi hizmetleri, bireylerin mahremiyetini ve dijital haklarını korumak için ulusal, bölgesel ve uluslararası düzeyde savunuculuk çabalarını desteklemeli ve kütüphane çalışanlarını bu konular üzerinde bilinçlendirmeye teşvik etmelidir.
- Kütüphane ve bilgi hizmetleri, elektronik gözetimi ve kullanıcıların kişisel verilerinin her türlü gayri meşru izlenmesini, toplanmasını veya mahremiyetlerini tehlikeye atacak ve bilgi arama, alma ve verme haklarını etkileyecek bilgi davranışlarını engelleyici önlemler almalıdır. Kurumsal ve kişisel bilgilerin toplanmasını sınırlamak için kontrol mekanizmalarını uygulamalıdır.
- Devletin, kullanıcıların verilerine erişimi ve veri gözetimi tamamen önlenemese de kütüphane ve bilgi hizmetleri, kullanıcıların bilgilerine veya iletişimlerine devlet tarafından izinsiz girilmesinin meşru ilkeler ve amaçlar çerçevesinde yapılmasını ve orantılı olmasını sağlamalıdır.
- Kütüphane ve bilgi hizmetleri, kullanıcıların mahremiyetini tehlikeye atabilecek kaynaklara, hizmetlere veya teknolojiye erişim sağladığında kullanıcıları sonuçlarından farkında olmaya teşvik etmeli, veri koruma ve mahremiyetin korunması konusunda rehberlik sağlamalıdır.
- Kütüphane ve bilgi hizmetleri, kullanıcılarının bilinçli seçimler yapma, meşru eylemlerde bulunma, iletişimlerinde ve internet üzerindeki hizmetlerin kullanımında riskleri ve faydaları bilme becerilerini desteklemelidir.
- Veri ve mahremiyetin korunması, kütüphane ve bilgi hizmeti kullanıcıları için medya ve bilgi okuryazarlığı eğitiminin bir parçası olarak dâhil edilmelidir. Kullanıcıların mahremiyetlerini korumak için kullanılacak araçlarla ilgili eğitimler düzenlenmelidir.
- Kütüphane ve bilgi uzmanlarının eğitimi, ağ ortamındaki veri ve mahremiyet koruma ilkelerini ve uygulamalarını içermelidir.

Bilgi güvenliği konusunu doğrudan ele alan bu belge dışında IFLA Etik Kuralları (2012) adıyla bilgi kullanımı konusunu kapsayan ikinci bir belge daha yayımlanıştır. Bu belgede, kütüphanecilerin ve bilgi çalışanlarının mesleki etik konularında bilinçlenmelerini ve politikalar oluşturabilmelerini sağlamak amacıyla rehberlik sağlamaktadır. Ayrıca, kütüphane çalışanlarının karşılaşabilecekleri etik ikilemleri çözebilmeleri için ilkeler sunmaktadır.

IFLA Etik Kuralları, bireysel kütüphaneciler ve bilgi çalışanları için mesleki profesyonellik konusunda rehberlik etmektedir. Bu belgede, kütüphanecilerin etik davranış standartları ve sorumlulukları vurgulanmaktadır. Kütüphanecilerin, kullanıcılarına hizmet sunarken dürüstlük, tarafsızlık, gizlilik ve saygı gibi değerlere bağlı kalmaları teşvik edilmektedir. Ayrıca, mesleklerine yönelik öz farkındalıklarını artırmaları konusunda hedefler sunulmaktadır. Kütüphanecilerin mesleki gelişimlerini desteklemek, etiksel düşünme ve refleksif uygulama becerilerini geliştirmek için ilke ve kuralların önerildiği bu belgede, kütüphanecilerin toplumun çeşitli gruplarına hizmet sunarken kültürel ve sosyal çeşitlilik konusunda duyarlı olmaları belirtilmektedir. Özetle, kütüphanecilerin ve bilgi çalışanlarının şeffaflık ve hesap verebilirlik ilkelerine uymalarını vurgulanmaktadır. Kütüphaneciler ve diğer bilgi çalışanları için etik değerlere dayalı bir çerçeve sunmaktadır.

Bu belgede, mesleki davranışın ve sorumlulukların temelini oluşturulmasını ve kütüphanecilik mesleğinin topluma olan değerini artırılmasını hedefleyen beş temel etik kural üzerinde durulmaktadır (IFLA, 2012):

- Bilgiye erişim,
- Bireyler ve topluma karşı sorumluluklar,
- Mahremiyet, gizlilik ve şeffaflık,
- Açık erişim ve telif hakları,
- Tarafsızlık, dürüstlük ve profesyonel beceriler,

Etik kurallarının tanımlandığı bu belgenin mahremiyet, gizlilik ve şeffaflık başlığı altında kütüphaneciler ve diğer bilgi çalışanlarının, kişisel mahremiyete ve kişisel verilerin korunmasına karşı tutumları belirtilmektedir. Kütüphaneciler ve diğer bilgi çalışanlarının kurumundaki bilgi ve bilgi varlıklarının şeffaflığını sağlamakla yükümlü olduğunu ve bu bilgi varlıklarının suiistimal, yolsuzluk ve ifşa edilmemesi konusunda kamu ve kişisel yararına göre hareket etmeleri gerektiği belirtilmektedir. Kütüphane ile kullanıcı arasındaki ilişkinin bir gizlilik ilişkisi içerisinde yürütülmesi ve kullanıcı verilerinin kütüphane işlemlerinin ötesinde paylaşılmamasını sağlamak için uygun önlemlerin alınması gerektiği vurgulanmaktadır.

Üniversite Kütüphanelerinde Bilgi Güvenliği Önlemleri

Üniversite kütüphaneleri, eğitim ve araştırma süreçlerinde önemli bir rol oynar ve geniş bir bilgi kaynağı sunarak öğrenci, öğretim elemanı ve araştırmacılara hizmet verir. Bu bilgi merkezlerinin bilgi varlıklarında saklanan ve erişilebilen bilgi ve belgelerin gizliliğinin, bütünlüğünün ve kullanılabilirliğinin koruması önemli bir hizmet disiplinin kasar. Üniversite

kütüphanelerinde, öğrenci ve araştırmacıların kişisel verileri, telif hakkıyla korunan yayınlar ve diğer hassas bilgilerin yetkisiz erişime karşı korunmasını sağlamak için güçlü gizlilik politikaları ve teknolojik önlemler geliştirmesi önemlidir. Bu kütüphanelerde depolanan bilgi ve belgelerin bütünlüğünün sağlanması, onların güvenilirliğini ve geçerliliğini artırır. Bu nedenle, üniversite kütüphaneleri, veri depolama ve iletişim sistemlerinde bütünlüğü sağlamak için güvenlik önlemleri uygulamalı ve buna yönelik süreçler geliştirmelidir. Ayrıca kütüphane kaynaklarına erişimin kolaylığı ve sürekliliği de kullanıcıların kütüphane kaynaklarına güvenli bir şekilde erişebilmelerini sağlamak için önemlidir. Üniversite kütüphaneleri, kullanıcılarının kimlik doğrulama, ağ güvenliği ve diğer teknik önlemlerini sağlayarak kullanılabilirliği desteklemeli ve kesintisiz hizmet sunmalıdır.

Bilgi güvenliği, risklerin varlığından kaynaklanır. Bu nedenle, gizlilik, bütünlük ve kullanılabilirlik, bilgi güvenliği temel ilkeleridir ve risklerin senteziyle ortaya çıkar. Bilgi ve belge yönetimi uygulamaları, belge yönetimi teknik ve yasal düzenlemeleri, belge oluşturma sürecinden erişim haklarının tanımlanmasına kadar tüm süreçte bu ilkeleri zorunlu kılar. Bilgi ve belgelerin gizliliği, bütünlüğü ve kullanılabilirliği açısından bilgi güvenliği yönetiminin önemi büyüktür. Bilgi güvenliği ilkeleri, kurumsal bilgi yönetimi hedeflerini somutlaştırırken, bilgi ve belge yönetimi prensipleri de bu somut hedefleri destekler (Güler ve Furat, 2022).

Tüm bilgi merkezi türlerinde olduğu gibi, üniversite kütüphanelerinde de bilgi güvenliğine yönelik çeşitli sorunlarla karşı karşıya kalınmaktadır. Bu sorunlar, gelişen teknolojiler, artan dijital kaynak kullanımı ve kullanıcıların çeşitli ihtiyaçlarından kaynaklanabilir. Özellikle, kütüphanelerde depolanan ve kullanıcılara sunulan dijital veriler, siber saldırganların hedefi olabilir. Bu nedenle üniversite kütüphaneleri, güçlü bir güvenlik altyapısı oluşturmalı ve siber saldırılara karşı korunma tedbirleri almalıdır.

Kolej ve Araştırma Kütüphaneleri Derneğinin (Association of College ve Research Libraries) "Yükseköğretim İçin Bilgi Okuryazarlığı Çerçevesi" metninde bilgi okuryazarlığının gizlilik ve kişisel bilgi güvenliği konularına dikkat etmeyi teşvik ettiği ifade edilmektedir. Bilgi okuryazarlığı eğitimi, bireylerin çevrimiçi etkileşimlerinde gizlilik ve güvenlik konularında bilinçli seçimler yapmalarına yardımcı olmayı hedefler. Bununla birlikte, bu alanda daha fazla vurgu yapılması ve bilgi okuryazarlığının bu konularda daha kapsamlı bir eğitim sunması gerektiği ifade edilmektedir. Gizlilik ve güvenliğin çevrimiçi ortamda önemli konular olduğu ve bireylerin bu konularda bilinçli olmaları, kişisel bilgilerini korumaları ve güvenli çevrimiçi davranışlar sergilemelerinin büyük önem taşıdığı belirtilmektedir. Bilgi okuryazarlığı, bireyleri bu konularda bilinçlendirmek ve onları güvenli ve sorumlu çevrimiçi kullanıcılar haline getirmek için önemli bir araç olarak kullanılması gerektiği vurgulanmaktadır (ACRL, 2016).

Üniversite kütüphaneleri, bilgi güvenliği yönetimine konusunda öncelikle bilgi güvenliği politikalarının belirlenmesine yönelik bir rol üstlenmelidir.. Bu politikalar, siber saldırılara karşı alınacak teknik önlemleri, veri güvenliği ve yedekleme prosedürlerini, kullanıcı bilgilerinin gizliliğini koruma yöntemlerini ve kullanıcıların bilgi güvenliği konusunda uyulması gereken kuralları kapsamaktadır. Bu politikaların düzenli olarak gözden geçirilmesi ve güncellenmesi önemlidir, çünkü bilgi güvenliği tehditleri sürekli olarak değişmekte ve gelişmektedir.

Üniversite kütüphaneleri, aynı zamanda teknolojik çözümlerle bilgi güvenliğini desteklemelidir. Bu kapsamda, güçlü güvenlik duvarları, antivirüs ve antimalware yazılımları, güvenli veri depolama sistemleri ve yetkilendirme mekanizmaları gibi teknolojiler kullanılabilir. Üniversite kütüphaneleri, düzenli veri yedeklemeleri yaparak veri kaybını önlemek için güvenilir depolama yöntemlerini benimsemelidir (Şişkin, 2020).Kullanıcı bilgilerinin gizliliği üniversite kütüphanelerinde büyük bir önem taşımaktadır. Kullanıcıların ödünç aldıkları materyalleri, araştırma kayıtlarını ve diğer kişisel bilgilerini gizli tutmak için gerekli önlemler alınmalıdır. Bu önlemler, gizlilik politikalarının etkin bir şekilde uygulanması, veri paylaşımının sınırlı tutulması ve kullanıcı bilgilerinin yetkisiz erişimlere karşı korunmasıyla sağlanır. Kullanıcıların güvenli ve güvenilir bir ortamda bilgiye erişebilmeleri için üniversite kütüphaneleri, gizlilik konusunda titizlikle hareket etmelidir (Henkoğlu, 2015).

Aşırı veri toplama ve kullanımı, bireysel kullanıcıların mahremiyetini tehdit etmekte ve başka sosyal ve yasal sonuçlara yol açmaktadır. İnternet kullanıcıları, büyük ölçekli veri toplama ve gözetlemenin farkında olduklarında beklenmedik sonuçlardan korktukları için davranışlarını sansürleyebilmektedir. Aşırı veri toplamanın toplum üzerinde caydırıcı bir etkisi olabilmekte ve algılanan bu tehdidin bir sonucu olarak bireyin konuşma ve ifade özgürlüğü hakkını daraltabilmektedir. İnsan Hakları Evrensel Beyannamesi'nin 19. maddesinde ifade edilen bilgiye erişim özgürlüğü ve ifade özgürlüğü, kütüphane ve bilgi mesleği için temel kavramlar olarak ifade edilmektedir. Gizlilik ise bu hakları sağlamanın ayrılmaz bir parçasıdır (IFLA, 2015).

Bilgi akışına yönelik özellikle eşitsizlik, yoksulluk ve umutsuzluğu artıran engelleri kaldırma amacıyla IFLA tarafından yayımlanan "internet bildirgesi"nde, kütüphane ve bilgi hizmetlerinin kullanıcılarının kişisel bilgilerinin, kullandıkları kaynakların ve hizmetlerin gizli kalmasını sağlamaya çalışma sorumluluğuna sahip kurumlar olması gerektiği bildirilmektedir (IFLA ve Kuhlenkamp, 2015). Ayrıca IFLA kütüphaneciler ve diğer bilgi çalışanları için yayımladığı etik kuralları bildirgesinde, kişisel mahremiyete saygıyı, kişisel verilerin korunmasını ve kullanıcı ile kütüphane arasındaki ilişkide gizliliği temel ilkeler olarak tanımlamaktadır (IFLA, 2012).

Üniversite kütüphanelerinde bilgi güvenliği yönetimi sistemlerinden sorumlu personelin düzenli olarak gizlilik denetimleri gerçekleştirmesi ve kullanılan teknolojilerinin gizlilik standartlarını karşıladığından emin olması gerekmektedir. Kütüphane sistemlerinin mümkün olan en az miktarda kullanıcı bilgisi toplayacak ve tutacak şekilde yapılandırılması gerekir. Bu bakımdan Amerikan Kütüphane Derneği (American Library Association), kütüphanelerdeki kurumsal ve kişisel bilgilerin güvenliği için birtakım öneriler sunmaktadır. Bunlar şu şekilde sıralanmaktadır (ALA, 2006):

- Kişisel olarak tanımlanabilir bilgilerin toplanma, izlenme, ifşa edilme ve dağıtılma derecesini sınırlandırılması,
- Gereksiz kayıtlar oluşturmaktan kaçınılması,
- Kişisel olarak tanımlanabilir bilgilere erişimi, yetkili işlevleri yerine getiren personelle sınırlandırılması,
- Verilerle ilgili günlükler, dijital kayıtlar, satıcı tarafından toplanan veriler ve sistem yedeklemelerin tutulması ve kitaplığın verimliliği ve yasal işleyişi için gerekli olmadıkça kişisel olarak tanımlanabilir bilgiler içeren kütüphane kullanım kayıtlarını imha edilmesi,
- Bilgi teknolojileri birimi veya otomasyon sistemleri tarafından işlenen veya tutulan kütüphane kullanım kayıtlarının bilgi güvenliği politikalarına uygun olarak ele alınması,
- Saklanması gereken kayıtların güvenli ortamlarda muhafaza edildiğinden emin olunması,
- Kişisel olarak tanımlanabilir bilgileri kamuya açık hale getiren kütüphane uygulamalarından ve prosedürlerinden kaçınılması,
- Tedarikçi sözleşmelerinin tüm veri ve kayıtların kütüphane kontrolünü garanti etmesinin sağlanması,
- Kütüphane kullanıcıları ve çalışanları hakkındaki bilgilerin nasıl toplandığını, saklandığını, paylaşıldığını, kullanıldığını ve imha edildiğini inceleyen gizlilik denetimlerinin gerçekleştirilmesi gerekir.

Araştırmanın Amacı, Önemi ve Problemi

Kütüphaneler, kullanıcılar ile zengin bilgi kaynakları arasında köprü konumundadır. Farklı platform ve kanallarla çeşitli kullanıcı profiline bilgi hizmeti sunmaktadır. Kütüphaneler sahip oldukları bilgileri erişime sunarken ya da diğer kurumlar ile iş birliği sağlarken çeşitli bilgi güvenliği risklerine maruz kalabilmektedir. Özellikle bünyelerindeki bilgi sistemlerine işlenen kurumsal ve kişisel kritik bilgilerin korunması bakımından önemli güvenlik açıklarına maruz kalabilmektedir. Bu nedenle kütüphanelerin bilgi güvenliği risklerini en alt düzeye indirilebilmeleri için iyi bir şekilde planlanmış bilgi güvenliği yönetim sistemini işler duruma getirmeleri gerekmektedir.

Bu bağlamda, araştırmanın temel amacı, Türkiye'deki üniversite kütüphanelerinde teknolojik ve kurumsal bilgi güvenliği önlemlerinin uygulanma düzeylerini belirlemek ve bu önlemlerin yeterliliği üzerine değerlendirmelerde bulunmaktır. Türkiye'de üniversite kütüphanelerinin bilgi güvenliği önlemleri ile ilgili mevcut durumun saptandığı ve tespitlere ilişkin değerlendirme ve önerilerin sunulduğu bu çalışma kütüphanecilik alanındaki konuya ilişkin farkındalığı artıracağı düşünülmektedir. Ayrıca araştırmada elde edilen bulgular ile Türkiye'de üniversite kütüphane yönetimlerinin bilgi güvenliği yönetimi ile ilgili eksikliklerini görmelerine ve bu eksiklerin giderilmesi konusunda uluslararası standartlarda uygun çalışmalar yürütebilmeleri konusunda katkı sağlaması beklenmektedir. Bu nedenle araştırma, üniversite kütüphanelerinin bilgi güvenliği konusuna odaklanmaları bakımından önemli bulunmaktadır.

Bilgi güvenliği yönetimi tüm kurumlar için önemli bir konudur. Kurumların bilgi sistemlerinde işlenen her bilginin üslendiği bir değer bulunmaktadır. Kurumsal faaliyetlerin gizliliği, bütünlüğü ve erişebilirliği açısından değerli olan bilgilerin korunması önem arz etmektedir. Özellikle de personel, kullanıcı veya müşterilere ait kişisel bilgilerin güvenliği daha da önemli bir durum haline gelmiştir. Bu bilgilerin gizliliğinin ifşası mahremiyet açısında birçok sorunu beraberinde getirmektedir. Üniversite kütüphaneleri de tüm kurumlarda olduğu gibi kurumsal ve kişisel birçok bilgiyi bilgi varlıklarına işlemektedir. Bu bilgilerin ne derecede güvenliğinin sağlandığı konusunda kullanıcılar, kurum yetkilileri ve diğer ilgili paydaşlar arasında tereddütler bulunmaktadır. Türkiye'de üniversite kütüphanelerine bilgi güvenliğine yönelik önlemlerin uygulanıp uygulanmadığı ve bu önlemlerin ne düzeylerde uygulandığı konusundaki tereddütlere açıklık getirebilmek amacıyla çalışma kapsamında aşağıdaki sorulara yanıt aranmıştır:

- Türkiye'de üniversite kütüphanelerinde teknolojik bilgi güvenliği önlemleri yeterli düzeyde uygulanmakta mıdır?
- Türkiye'de üniversite kütüphanelerinde kurumsal bilgi güvenliği önlemleri yeterli düzeyde uygulanmakta mıdır?

Yöntem

Türkiye'de üniversite kütüphanelerinde bilgi güvenliği tehditlerine karşı uygulanan teknik ve kurumsal önlemlerin düzeyini belirlemek için verilerin toplanmasını amaçlayan bu çalışmada tarama yönteminden yararlanılmıştır. Tarama yöntemi geçmişte ya da halen var olan olayların, olguların, nesnelerin, kurumların veya çeşitli durumların kendi koşulları içerisinde olduğu gibi tanımlanmasını ya da belli özelliklerinin neler olduğunun ortaya çıkarılmasını amaçlayan araştırma yaklaşımıdır (Karasar, 2019; Eşitti, 2018). Tarama araştırmalarında genellikle geniş bir kitleden araştırmacı tarafından belirlenen cevap seçenekleri kullanılarak bilgi toplanır. Genellikle tarama

araştırmalarında araştırmacılar, görüşlerin ve özelliklerin neden kaynaklandığından çok örneklemdeki bireyler açısından nasıl dağıldığıyla ilgilenmektedir (Fraenkel ve Wallen, 2006).

Araştırmanın evreni, Türkiye'de üniversite kütüphanelerinde bilgi işlem sistemlerinin uygulayıcısı ve karar vericisi olan daire başkanları, birim sorumluları, öğretim görevlileri, kütüphaneciler ve bilgi işlem uzmanlarından oluşmaktadır. Evrendeki üniversite kütüphanelerindeki tüm görevlilerin çalışmaya olan katkılarının homojen bir biçimde sağlanabilmesi ve çalışmanın amacına katkı sağlayacak bilgi açısından zengin ve nitelikli ölçütlere sahip personelin belirlenmesi için olasılıklı (tesadüfi) olmayan bir örnekleme yaklaşımı olan "amaca dayalı (yargısal) örnekleme" yöntemi kullanılmıştır (Büyüköztürk ve diğerleri, 2022; Güriş ve Astar, 2014; Yazıcıoğlu ve Erdoğan, 2014). Bu yöntem ile evren parametresindeki benzer özellikteki personelin seçimi bizzat araştırmacı tarafından özenle gerçekleştirilerek çalışmanın örneklem grubu oluşturulmuştur.

Bu itibarla, Türkiye'de 130'u devlet, 74'ü vakıf ve 4'ü vakıf yüksekokulu olmak üzere toplamda 208 üniversiteden (YÖK, 2022) 9 üniversite kütüphanesi hariç (merkezi kütüphaneye veya uzman bir kütüphane personeline sahip olmayan 2 devlet üniversitesi ve 3 vakıf meslek yüksekokulu, Kahramanmaraş merkezli iki büyük deprem felaketinden etkilenen üç devlet üniversitesi ve araştırmaya katılım sağlamak istemeyen bir devlet üniversitesi) 199 üniversite kütüphanesi araştırmanın kapsamına dâhil edilmiştir.

Veri toplama aracı olarak, araştırmanın amaç ve planına göre düzenlenmiş sorulardan oluşan bir anket formu geliştirilmiştir. Çalışmanın problem durumuna ve amacına uygun sorularının belirlenmesi, taslak formun oluşturulması, uzman görüşlerinin alınması, ön uygulama, analizler ve son şeklinin verilmesi gibi belirli anket geliştirme aşamalarından (Büyüköztürk ve diğerleri, 2022) geçilerek güvenirliği ve kapsam geçerliliği sağlanan anket formunda, teknolojik (donanım, yazılım, ağ, veri, fiziksel çevre) ve kurumsal (güvenlik politikası, prosedürü, idari araçları ve farkındalık çalışmaları) bilgi güvenliği içerisinde değerlendirilen 9 kategori altında toplam 104 maddeden oluşan likert tipi bilgi güvenliği önlem maddesi bulunmaktadır. Geliştirilen bu anket formu, 199 üniversite kütüphanesi çalışanları arasından belirlenen örneklem gruba uygulanmıştır.

Anketteki maddelerin uygulama düzeylerine ilişkin durumu istatistiksel olarak veren derecelendirme seçenekleri "hiç uygulanmamaktadır", "kötü düzeylerde uygulanmaktadır", "orta düzeylerde uygulanmaktadır" ve "iyi düzeylerde uygulanmaktadır" olarak değerlendirilmiştir. Ayrıca teknolojik ve kurumsal güvenlik önlemlerine ilişkin herhangi bir bilgisi olmayan ya da çalıştığı kütüphanede varlığı veya uygulanmasına ilişkin tereddüt yaşayan katılımcıların cevabının diğer

katılımcıların cevaplarındaki niteliği etkilememesi veya o maddeyi boş bırakmaması için her maddeye "fikrim yok" seçeneği de eklenmiştir. "Fikrim yok" seçeneği, bir katılımcının belirli bir madde hakkında yeterli bilgiye sahip olmadığını kabul etmesini ve diğer katılımcıların cevaplarını etkilememek veya o maddenin boş bırakılmaması sağlamak amacıyla araştırmacılar tarafından önerilen bir çözüm seçeneğidir (Dursun ve Alnıaçık, 2019; Krosnick ve Fabrigar, 1997). Araştırma kapsamında uygulanan anket formundan elde edilen veriler IBM SPSS 26.0 programı ile analiz edilerek değerlendirilmiştir. Türkiye'de üniversite kütüphanelerinde uygulanan bilgi güvenliği önlemlerinin düzeylerine ilişkin katılımcılardan elde edilen tanımlayıcı verilerin frekans değerleri tablolar halinde değerlendiriliştir.

Bulgular

Türkiye'de üniversite kütüphanelerinde teknolojik ve kurumsal bilgi güvenliği önlemlerinin uygulanıp uygulanmadığı, uygulanıyorsa ne düzeylerde uygulandığını tespit etmek amacıyla katılımcıların yanıtladığı anket formundan elde edilen veriler çalışmanın soruları bağlamında aşağıda yarı ayrı incelenmiştir.

Katılımcıların Tanımlayıcı Profillerine İlişkin Bulgular

Araştırmaya katılanların cinsiyeti, eğitim durumu, çalıştığı üniversitenin türü, üniversite kütüphanesindeki görevi ve iş tecrübesi gibi demografik bilgileri Tablo 1'de verilmiştir.

Tablo 1: Katılımcılara ait demografik bilgiler

		Devlet Üniversitesi		Vakıf Üniversitesi		Toplam	
		f	*%*	*f*	*%*	*f*	*%*
Cinsiyet	Kadın	63	50,8	54	72,0	117	58,8
	Erkek	61	49,2	21	28,0	82	41,2
Eğitim Durumunuz	Ön Lisans	0	0,0	1	1,3	1	0,5
	Lisans	79	63,7	42	56,0	121	60,8
	Lisansüstü (Yüksek Lisans/Doktora)	45	36,3	32	42,7	77	38,7
Mezuniyet Programı	Bilgi ve Belge Yönetimi vb.	106	85,5	61	81,3	167	83,9
	Bilgisayar / Bilişim / Yazılım	2	1,6	4	5,3	6	3,0
	Diğer	16	12,9	10	13,3	26	13,1
Görev	Daire Başkanı	5	4,0	15	20,0	20	10,1
	Şube Müdürü	10	8,1	2	2,7	12	6,0
	Öğretim Görevlisi	22	17,7	0	0,0	22	11,1
	Kütüphaneci	80	64,5	54	72,0	134	67,3
	Bilgisayar / Bilgi İşlem Uzmanı	4	3,2	1	1,3	5	2,5
	Diğer	3	2,4	3	4,0	6	3,0
İş Tecrübesi	1 - 5 yıl	31	25,0	40	53,3	71	35,7
	6 - 10 yıl	44	35,5	15	20,0	59	29,6
	11 - 15 yıl	29	23,4	8	10,7	37	18,6
	16 - 20 yıl	14	11,3	4	5,3	18	9,0
	21 yıl ve üzeri	6	4,8	8	10,7	14	7,0
Üniversite Türü	Devlet Üniversitesi	124	100,0	0	0,0	124	62,3
	Vakıf Üniversitesi	0	0,0	75	100,0	75	37,7
	Toplam	**124**	**100,0**	**75**	**100,0**	**199**	**100,0**

Tablo 1'deki veriler, her devlet ve vakıf üniversitesinden çalışmaya katılım sağlayan personelin istihdam profilleri arasında bazı farklılıkların olduğunu göstermektedir. Ankete, 199 üniversite kütüphanesinin her birinden bir personelin katılımı sağlanmıştır. Bu yönüyle katılımcılardan elde edilen tüm veriler Türkiye'de üniversite kütüphanelerinin bütününü temsil etmektedir.

Katılımcıları demografik yapısına ilişkin veriler ayrı ayrı incelendiğinde, devlet üniversitelerindeki katılımcıların kadın oranı %50,8 iken, vakıf üniversitelerinde %72,0'dir. Genel olarak, her iki üniversitede de kadın çalışan oranı erkek çalışan oranından daha yüksektir.

Katılımcılardan lisans derecesine sahip olanlar, her iki üniversitede de en yüksek orana sahiptir. Ön lisans ve lisansüstü eğitim düzeylerinde ise küçük farklar vardır.

Katılımcıların her iki üniversite türünde de en yaygın mezuniyet programının Bilgi ve Belge Yönetimi veya benzeri programlar olduğu ve bunu Bilgisayar/Bilişim/Yazılım programlarının takip ettiği görülmektedir. Bu durum çalışmanın örneklem seçiminin amaca uygun olarak yapıldığını desteklemektedir.

Katılımcıların mezun oldukları program verilerinde "diğer" seçeneği içerisinde lisans derecesini Bilgi ve Belge Yönetimi, Kütüphanecilik, Arşivcilik ve Dokümantasyon Programlarının herhangi birinden mezun olup yüksek lisans derecelerini farklı programlarda tamamlamış kütüphaneciler ile birlikte öğretmenlik, işletme, iktisat, halkla ilişkiler ve mühendislik programlarının lisans derecesinden mezun olan katılımcılar bulunmaktadır. Kütüphanedeki görevi bakımından "diğer" seçeneğini işaretleyen katılımcıların ise şef, idari ve büro personeli olarak görev yaptıklarını belirtmişlerdir.

Katılımcılar arasında Kütüphaneci olanlar, her iki üniversitede de en yüksek görev grubunu oluştururken, daire başkanları ve şube müdürleri ikinci en yüksek grup arasında yer almıştır.

Katılımcıların çoğunlukla 6-10 yıl ve 1-5 yıl arasındaki iş tecrübesine sahip çalışanlardan oluştuğu görülmektedir. Kütüphanecilik alanında iş tecrübesi olan bu katılımcıların belirli bir yetkinliğe, eğitim ve farkındalığa sahip olabilmesi, bu çalışmanın verilerinin sağlıklı ve geçerli olması açısından yeterli bulunmaktadır.

Teknolojik Bilgi Güvenliği Önlemlerinin Uygulanma Düzeyleri

Bu başlık altında, üniversite kütüphanelerinde teknolojik bilgi güvenliği önlemlerinden donanım güvenliği (Tablo 2), yazılım güvenliği (Tablo 3), ağ güvenliği (Tablo 4), veri güvenliği (Tablo 5), ve fiziksel-çevresel güvenlik (Tablo 6) kategorilerde yer alan önlem maddelerinin uygulama düzeyleri hakkında katılımcıların görüşlerine ilişkin frekans dağılımları verilmiştir.

Tablo 2: Donanım güvenliği önlemlerinin uygulama düzeyleri

	Donanım Güvenliği Önlemleri Maddeleri		*Uygulanma Düzeyi*				*Fikrim yok*
			Hiç	*Kötü*	*Orta*	*İyi*	
1	Veri işleme, depolama ve iletme yeteneğine sahip tüm donanımların güncel envanteri tutulmakta ve kullanım tahsisleri yapılmaktadır.	*f*	2	5	43	138	11
		%	1,0	2,5	21,6	69,3	5,5
2	Kütüphane envanterindeki tüm cihaz ve taşınabilir ortamlar, kaybolma veya çalınma riskine karşı şifrelenmektedir.	*f*	3	21	55	108	12
		%	1,5	10,6	27,6	54,3	6,0
3	Kritik bilgi içeren taşınabilir cihaz ve ortamlar güvenli şekilde saklanmakta ve kurum dışına çıkarılmasına izin verilmemektedir.	*f*	1	9	33	147	9
		%	0,5	4,5	16,6	73,9	4,5
4	Kütüphane envanterinden çıkarılan donanımların veri depolama ünitelerindeki veri ve bilgiler geri getirilmeyecek şekilde silinmektedir	*f*	6	7	41	90	55
		%	3,0	3,5	20,6	45,2	27,6
5	Kullanım ömrünü tamamlamış veri depolama üniteleri (HDD, SSD, harici bellek, USB, disk vb.) güvenli bir biçimde imha edilmektedir.	*f*	11	15	31	85	57
		%	5,5	7,5	15,6	42,7	28,6
6	Yeni tedarik edilen sabit diskler veri kurtarmaya imkân sağlamayacak bir şekilde biçimlendirilerek sisteme dâhil edilmektedir	*f*	10	15	36	70	68
		%	5,0	7,5	18,1	35,2	34,2
7	Bilgi içeren tüm cihaz ve ortamların ısı, nem ve elektromanyetik gibi tehditlere maruz kalamaması için çevresel önlemler alınmaktadır.	*f*	9	17	53	101	19
		%	4,5	8,5	26,6	50,8	9,5
8	Onarım veya güncelleme nedenleri ile kurum dışına çıkarılacak cihaz ve ortamlardaki kritik bilgiler geri getirilmeyecek şekilde silinmektedir.	*f*	12	14	36	74	63
		%	6,0	7,0	18,1	37,2	31,7
9	Nesnelerin interneti (IoT cihazları) ile ilgili kurulum, imha ve yeniden kullanıma alma gibi işlemler yetkili personelce yapılmaktadır.	*f*	5	9	31	117	37
		%	2,5	4,5	15,6	58,8	18,6

Tablo 2'deki veriler incelendiğinde, üniversite kütüphanelerindeki donanım varlılarının güvenliğine ilişkin önlemelerin bir kısmının (1. madde %69,3, 2. madde %54,3, 3. madde %73,9, 7. madde %50,8, 9. madde %58,8) iyi düzeylerde uygulandığı fakat önlemlerin uygulanma düzeylerine genel olarak bakıldığında yeterli seviyelerde gerçekleşmediği anlaşılmaktadır. Özellikle de "kritik bilgi içeren taşınabilir cihaz ve ortamların güvenli şekilde saklanması ve kurum dışına çıkarılmasına izin verilmemesi ile ilgili uygulamanın diğer donanım önlemlerine göre daha üst seviyelerde uygulandığı belirlenmiştir.

Bu kategoride yer alan önlemler arasında "onarım veya güncelleme nedenleri ile kurum dışına çıkarılacak cihaz ve ortamlardaki kritik bilgilerin geri getirilmeyecek şekilde silinmesi" ve "yeni tedarik edilen sabit disklerin veri kurtarmaya imkân sağlamayacak bir şekilde biçimlendirilerek sisteme dâhil edilmesi" önlemlerinin yoğun olarak uygulanmadığı görülmüştür. Ayrıca donanım önlemlerinin uygulanmasına ilişkin herhangi bir fikir sunamayan katılımcıların bazı maddelerde (4. madde %27,6; 5. madde %28,6; 6. madde %34,2; 8. madde %31,7) yoğunlaştığı görülmüştür. Bu nedenle

donanım güvenliği ile ilgili bu önlemlerin üniversite kütüphanelerinde yeterli düzeylerde uygulanmadığı veya bunlara ilişkin bilgilendirmelerin eksik olduğu söylenebilir

. Bu durum üniversite kütüphanelerinde donanım güvenliği önlemlerine ilişkin güvenlik tehdidi risklerini arttırabileceğini göstermektedir.

Tablo 3: Yazılım güvenliği önlemlerinin uygulanma düzeyleri

Yazılım Güvenliği Önlemleri Maddeleri			*Uygulanma Düzeyi*				*Fikrim yok*
			Hiç	*Kötü*	*Orta*	*İyi*	
10	Yazılımların adı, sürümü, yayımcısı, sözleşme, lisans ve edinim tarihi gibi bilgilerden oluşan detaylı yazılım envanteri tutulmaktadır.	*f*	2	6	32	137	22
		%	1,0	3,0	16,1	68,8	11,1
11	Yazılım ve uygulamaların kurulumu, yapılandırılması ve güncellemesi yetkili personel tarafından yapılacak şekilde kısıtlanmaktadır.	*f*	1	6	39	140	13
		%	0,5	3,0	19,6	70,4	6,5
12	Yetkisiz yazılım kullanımını tespit etmek ya da önlemek için beyaz liste uygulaması gibi kontroller kullanılmaktadır.	*f*	7	13	35	67	77
		%	3,5	6,5	17,6	33,7	38,7
13	Bilinen ya da şüphelenilen zararlı web sitelerini tespit etmek ve önlemek için kara liste uygulaması gibi kontroller uygulanmaktadır.	*f*	7	9	32	93	58
		%	3,5	4,5	16,1	46,7	29,1
14	Bilgisayarların ve bilişim sistemlerinin korunması ve taranması için zararlı yazılım tespit uygulamaları (Norton, Mcafee, Bitdefender vb.) kullanılmaktadır.	*f*	2	8	28	140	21
		%	1,0	4,0	14,1	70,4	10,6
15	Zararlı yazılım ve saldırı tespit gibi koruma uygulamaları, kullanıcılar tarafından devre dışı bırakılmayacak şekilde yapılandırılmaktadır.	*f*	2	9	39	106	43
		%	1,0	4,5	19,6	53,3	21,6
16	Kritik veri işleyen sistem yazılımları, onaylanmamış dosya yüklemelerine ve yetkisiz değişikliklere karşı düzenli olarak gözden geçirilmektedir.	*f*	5	13	30	99	52
		%	2,5	6,5	15,1	49,7	26,1
17	Felaket, saldırı, sistem arızası ve kullanıcı hatası kaynaklı veri / bilgi kayıplarına karşı yazılım ve uygulama yedeklemeleri yapılmaktadır.	*f*	5	6	33	122	33
		%	2,5	3,0	16,6	61,3	16,6
18	Olası güvenlik ihlallerini belirlemek ve kanıt üretmek için bilgi sistemlerinde gerçekleştirilen kullanıcı işlemleri düzenli olarak gözden geçirilmektedir.	*f*	6	6	35	102	50
		%	3,0	3,0	17,6	51,3	25,1
19	Bilgi sistemlerinde tespit edilen zararlı yazılımlar ve saldırılar üst yönetime ve bilgi işlem birimine iletilmektedir.	*f*	2	6	28	137	26
		%	1,0	3,0	14,1	68,8	13,1
20	Bilgisayarlar, taşınabilir ortamları zararlı yazılım taramasından otomatik olarak geçirilecek ve otomatik olarak çalıştırılmasına izin vermeyecek şekilde yapılandırılmaktadır.	*f*	4	5	40	105	45
		%	2,0	2,5	20,1	52,8	22,6
21	Kurumsal ve kişisel bilgi içeren uygulamalara ve yazılımlara, kişisel cihaz ve ortamların bağlanmasına izin verilmemektedir.	*f*	7	16	49	100	27
		%	3,5	8,0	24,6	50,3	13,6

Tablo 3'teki veriler incelendiğinde, üniversite kütüphanelerindeki yazılım varlıklarının güvenliğine ilişkin önlemelerin çoğunluğunun (10. madde %68,8; 11. madde %70,4; 14. madde %70,4; 17. madde %61,3; 19. madde %68,8) iyi düzeylerde uygulandığı görülmektedir. Özelliklede "yazılım ve uygulamaların kurulumu, yapılandırılması ve güncellemesinin yetkili bir personel tarafından yapılması" ve "bilgisayarların ve bilişim sistemlerinin korunması ve taranması için zararlı yazılım tespit

uygulamalarının (Norton, Mcafee, Bitdefender vb.) kullanılması" önlemlerinin daha iyi düzeylerde uygulandığı belirlenmiştir.

Bu güvenlik kategorisinde "yetkisiz yazılım kullanımını tespit etmek ya da önlemek için beyaz liste uygulaması" ve "bilinen ya da şüphelenilen zararlı web sitelerini tespit etmek ve önlemek için kara liste uygulaması" gibi kontrollerin uygulanmasında zayıflıkların olduğu tespit edilmiştir. Ayrıca birçok yazılım önleminin uygulanması konusunda (12. madde %38,7; 13. madde %29,1; 15. madde %21,6; 16. madde %26,1; 18. madde %25,1; 20. madde %22,6) yüksek oranlarda katılımcının fikir sahibi olmadığı görülmüştür. Bu nedenle yazılım güvenliği önlemlerine ilişkin uygulamaların üniversite kütüphanelerinde uygulanmasına ilişkin eksikliklerin olduğu veya personel arasında bu konuda farkındalığın gelişmediği söylenebilir.

Tablo 4: Ağ güvenliği önlemlerinin uygulanma düzeyleri

	Ağ Güvenliği Önlemleri Maddeleri		***Uygulanma Düzeyi***				***Fikrim yok***
			Hiç	***Kötü***	***Orta***	***İyi***	
22	Ağ hizmetlerinin güvenliği için kullanıcı kimlik doğrulama ve şifreleme gibi ağ bağlantısı kontrolleri uygulanmaktadır.	*f*	1	3	23	162	10
		%	0,5	1,5	11,6	81,4	5,0
23	Ağlar; personel, öğrenci gibi kullanıcı seviyelerine ve bilgi sistemlerine göre birbirinden ayrılmaktadır. (Personel / öğrenci ağı, sunucu / istemci ağı vb.)	*f*	4	6	24	154	11
		%	2,0	3,0	12,1	77,4	5,5
24	Misafir cihazlarının yalnızca misafir ağına erişimlerinin olduğu genel ağdan izole edilmiş ayrı bir ağ kullanılmaktadır.	*f*	10	11	29	120	29
		%	5,0	5,5	14,6	60,3	14,6
25	Bilişim sistemlerine yönelik saldırıları tespit etmek ve engellemek için ağ tabanlı saldırı tespit sistemleri kullanılmaktadır.	*f*	3	3	26	107	60
		%	1,5	1,5	13,1	53,8	30,2
26	Onaylanmayan ve erişimi yasak olan web sitelerinin bağlantısını engellemek için ağ tabanlı URL filtrelemesi uygulanmaktadır.	*f*	1	5	26	129	38
		%	0,5	2,5	13,1	64,8	19,1
27	Ağlar arasında iletişim güvenliğini sağlamak ve uzak kullanıcıları kurum ağlarına güvenli şekilde bağlamak için güvenlik duvarı gibi güvenli ağ geçitleri kullanılmaktadır.	*f*	2	4	30	141	22
		%	1,0	2,0	15,1	70,9	11,1
28	Kritik bilgi işleyen bilgisayar ve diğer sistemlerin wifi, bluetooth, 3G gibi kablosuz ve kablolu ağ bağlantıları sınırlandırılmakta veya engellenmektedir.	*f*	10	8	24	94	63
		%	5,0	4,0	12,1	47,2	31,7
29	Elektronik bilgi iletiminde, elektronik haberleşme ile ilgili iş süreçleri, yasal ve güvenlik kontrol gereksinimleri dikkate alınmaktadır.	*f*	3	1	32	124	39
		%	1,5	0,5	16,1	62,3	19,6
30	Kurumun ağ yönetim sorumlularının bilgisi olmadan ağa switch, hub, modem veya access point gibi aktif cihazlar dâhil edilmemektedir.	*f*	4	3	26	125	41
		%	2,0	1,5	13,1	62,8	20,6
31	Ağ teknolojisi ile çalışan telefon, faks, fotokopi gibi cihazların kayıtları tutulmakta ve kullanıcı sorumluları belirlenmektedir.	*f*	4	4	33	121	37
		%	2,0	2,0	16,6	60,8	18,6
32	Kurum ağına bağlanan kullanıcılara ait donanımların erişimleri, port seviyesinde kontrol edilmekte ve zararlı donanımlar engellenmektedir.	*f*	2	6	24	108	59
		%	1,0	3,0	12,1	54,3	29,6

Tablo 4'teki veriler incelendiğinde, üniversite kütüphanelerindeki ağ varlıklarının güvenliğine ilişkin önlemelerden 28. maddedeki (%47,2) önlem dışında diğer önlemlerin %53,3 ile %81,4 oranları arasında iyi düzeylerde

uygulandığı bulgusuna ulaşılmıştır. Özelliklede "ağ hizmetlerinin güvenliği için kullanıcı kimlik doğrulama ve şifreleme gibi ağ bağlantısı kontrollerinin uygulanması", "ağların personel, öğrenci gibi kullanıcı seviyelerine ve bilgi sistemlerine göre birbirinden ayrılması" ve "ağlar arasında iletişim güvenliğini sağlamayı ve uzak kullanıcıları kurum ağlarına güvenli şekilde bağlanmasını sağlayan güvenlik duvarı gibi güvenli ağ geçitlerinin kullanılması" önlemlerinin daha yoğun düzeylerde kullanıldığı belirlenmiştir.

Bu kategoride yer alan güvenlik önlemlerinden "kritik bilgi işleyen bilgisayar ve diğer kablosuz ve kablolu ağ bağlantılarının sınırlandırılması" önleminin uygulanma düzeyinin diğerlerine göre daha düşük düzeylerde uygulandığı görülmüştür. Bu önleme ilişkin %31,7 oranında katılımcının fikir sahibi olmadığını belirtmesi, bu maddedeki önlemin diğerlerine göre iyi oranlarda çıkmamasına sebep olduğu söylenebilir. Ayrıca "bilişim sistemlerine yönelik saldırıları tespit etmek ve engellemek için ağ tabanlı saldırı tespit sistemlerinin kullanılması (%30,2)" ve "kurum ağına bağlanan kullanıcılara ait donanımların erişimlerinin port seviyesinde kontrol edilmesi ve zararlı donanımların engellenmesi (%29,6) önlemlerine ilişkin katılımcıların yüksek oranlarda fikir sunmadığı, bu nedenle uygulama düzeylerinin de diğer önlemlere göre düşük oranlarda gerçekleştiği belirlenmiştir. Ağ güvenliği önlemlerinin hiç uygulanmamasına ilişkin verilerin ise %0,5 ile %5,0 oranları arasında olması, bu önlemlerin büyük çoğunlukla uygulandığını fakat yeterli düzeylerde uygulanmadığını göstermektedir.

Tablo 5: Veri güvenliği önlemlerinin uygulanma düzeyleri

	Veri Güvenliği Önlemleri Maddeleri		*Uygulanma Düzeyi*				*Fikrim yok*
			Hiç	*Kötü*	*Orta*	*İyi*	
33	Bilgi yaşam döngüsü içerisinde işlenen, depolanan, iletilen ve imha edilen kritik bilgiler belirlenmekte ve kayıtları tutulmaktadır.	*f*	4	8	42	105	40
		%	2,0	4,0	21,1	52,8	20,1
34	Bilgiler; değeri, kritikliği ve gizliliği gibi hassasiyetlere göre sınıflandırılmakta ve uygun sınıflandırma etiketi verilmektedir.	*f*	5	10	39	104	41
		%	2,5	5,0	19,6	52,3	20,6
35	Bilgisayar ve taşınabilir ortamlarda (HDD, SSD, harici bellek vb.) muhafaza edilen kritik bilgiler şifrelenmektedir.	*f*	7	9	47	92	44
		%	3,5	4,5	23,6	46,2	22,1
36	Kritik ve değerli bilgiler, depolama ortamı hasarı ve kaybı riskine karşı farklı bir güvenli ortamda da yedeklenmekte ve saklanmaktadır.	*f*	4	7	39	118	31
		%	2,0	3,5	19,6	59,3	15,6
37	Kullanım dışı kalan bilgisayar ve depolama ortamlarındaki kritik bilgiler, yetkili personelce güvenli şekilde silinmektedir.	*f*	4	6	41	109	39
		%	2,0	3,0	20,6	54,8	19,6
38	Kritik bilgiye ve bilgi işleme sistemlerine erişimler, en az ayrıcalık ilkesine göre yetkilendirilen personelle kısıtlanmaktadır.	*f*	2	6	38	115	38
		%	1,0	3,0	19,1	57,8	19,1
39	Kişisel bilgilerin erişim yetkilendirmeleri önceden belirlenmiş ilke ve yöntemlere göre verilmektedir.	*f*	0	10	35	120	34
		%	0,0	5,0	17,6	60,3	17,1
40	Bilgi sistemlerindeki kullanıcı bilgilerinin tedarikçilerce ihlal edilmemesi karşılıklı sözleşme ile koruma altına alınmaktadır.	*f*	3	6	35	103	52
		%	1,5	3,0	17,6	51,8	26,1
41	Personel, tedarikçi ve kullanıcıların bilgi sistemlerindeki bilgilere erişim yetkileri, düzenli aralıklarla gözden geçirilmekte ve ilişkileri sone erdiğinde kaldırılmaktadır.	*f*	2	9	30	121	37
		%	1,0	4,5	15,1	60,8	18,6
42	Bilgi sistemi ve hizmetlerinden yararlanacak her kullanıcı için ayrı bir hesap tanımlanmakta ve ortak hesap kullanımına izin verilmemektedir.	*f*	1	6	30	139	23
		%	0,5	3,0	15,1	69,8	11,6
43	Kullanıcılardan kişisel bilgilerin sistemler arasında veya gerekli hallerde kurum içinde kullanılacağı ile ilgili açık rıza onayı alınmaktadır.	*f*	7	10	37	110	35
		%	3,5	5,0	18,6	55,3	17,6
44	Bilgi sistemlerine kullanıcı kayıtlarında kişisel bilgilerin (T.C. numarası, doğum tarihi vb. üyelik numarası ve şifre olarak kullanılmamaktadır.	*f*	8	23	40	99	29
		%	4,0	11,6	20,1	49,7	14,6
45	Bilgi sistemlerine varsayılan kullanıcı hesap parolalarıyla giriş izni verilmemekte, güçlü parola kullanımı uygulanmaktadır.	*f*	7	20	37	111	24
		%	3,5	10,1	18,6	55,8	12,1
46	Kritik bilgilerin kurum dışına aktarımı sadece yetkili kullanıcı hesaplarıyla yapılmaktadır.	*f*	3	5	31	122	38
		%	1,5	2,5	15,6	61,3	19,1
47	Veri tabanlarının güvenilir bir şekilde yönetimini sağlamak için YETKİM gibi merkezi kimlik doğrulama sistemleri kullanılmaktadır.	*f*	11	10	29	89	60
		%	5,5	5,0	14,6	44,7	30,2

Tablo 5'teki veriler incelendiğinde, üniversite kütüphanelerindeki veri varlıklarının güvenliğine ilişkin önlemelerden 35. madde (%46,2), 44. madde (%49,7) ve 47. madde (%44,7), önlemleri dışındaki çoğu önlemin %51,8 ile %69,8 oranları arasında iyi düzeylerde uygulandığı sonucuna ulaşılmıştır. Özellikle de "bilgi sistemi ve hizmetlerinden yararlanacak her kullanıcı için ayrı bir hesabın tanımlanması ve ortak hesap kullanımına izin verilmemesi" bu kategori içerisinde değerlendirilen en yüksek uygulanma düzeyine sahip önlem olduğu görülmüştür.

Bu kategorideki güvenlik önlemlerinin uygulanması konusunda %11,6 ile %30,2 oranları arasında katılımcının herhangi bir fikir sunmadıkları görülmüştür. Veri güvenliği önlemlerinin uygulanması katılımcının bir fikir sahibi olmaması, bu gruptaki önlemlerin uygulanması konusunda risk oluşturabilir. Bu bulgular, veri güvenliği önlemlerinin genel olarak ortalama düzeylerde uygulandığını fakat bu konudaki önlemlere ilişkin önemli derecede iyileştirmelere ve düzeltmelere ihtiyaç olduğu söylenebilir.

Tablo 6.1: Fiziksel ve çevresel güvenlik önlemlerinin uygulanma düzeyleri

	Fiziki ve Çevresel Güvenlik Önlemleri Maddeleri		***Uygulanma Düzeyi***				***Fikrim yok***
			Hiç	***Kötü***	***Orta***	***İyi***	
48	Kütüphanenin ana giriş ve çıkış kapıları güvenlik birimi personeli ya da kartlı, turnikeli, RFID gibi kapı sistemleri ile denetlenmektedir.	*f*	14	9	22	154	0
		%	7,0	4,5	11,1	77,4	0,0
49	Kritik bilgi barındıran alanların fiziksel güvenlik sınırları belirlenmekte ve kapı, pencere gibi kısımlar güvenlik mekanizmaları ile korunmaktadır.	*f*	8	20	40	126	5
		%	4,0	10,1	20,1	63,3	2,5
50	Kütüphanede güvenlik kontrollerini sağlayacak yetkinliğe sahip yeterli sayıda güvenlik personeli çalıştırılmaktadır.	*f*	30	41	44	83	1
		%	15,1	20,6	22,1	41,7	0,5
51	Kütüphanenin iç ve dış alanları güvenlik kameraları ile takip edilmektedir.	*f*	5	15	36	141	2
		%	2,5	7,5	18,1	70,9	1,0
52	Ziyaretçilerin (kurye, firma yetkilisi, tesisatçı, teknik ekip vb. giriş ve çıkışları kayıt altına alınmakta ve sadece ilgili amaçları için erişim izni verilmektedir.	*f*	22	28	38	108	3
		%	11,1	14,1	19,1	54,3	1,5
53	Ziyaretçilerin kabul edileceği alanlar personel ve kullanıcı çalışma alanlarından ayrı bir bölgede konumlandırılmaktadır.	*f*	37	38	42	82	0
		%	18,6	19,1	21,1	41,2	0,0
54	Refakat edilmeyen ziyaretçilere yaka kısımlarında görünür şekilde ziyaretçi kartı takma zorunluluğu uygulanmaktadır.	*f*	68	44	30	53	4
		%	34,2	22,1	15,1	26,6	2,0
55	Kritik bilgilerin işlendiği veya saklandığı alanlara erişim, uygun kontroller (kartlı / şifreli erişim vb.) uygulanarak yetkili kişiler ile sınırlandırılmaktadır.	*f*	13	22	35	120	9
		%	6,5	11,1	17,6	60,3	4,5
56	Kütüphane binasına ait pencereler, kapılar ve bahçe alanları, demir parmaklık, çit, kilit, tel örgü gibi dış güvenlik unsurlarıyla kontrol edilmektedir.	*f*	26	31	46	95	1
		%	13,1	15,6	23,1	47,7	0,5
57	Bilgi sistemlerinin enerji ve iletişim hizmetlerini taşıyan kablolar, dinleme ve hasara karşı kablo kanalı ve izolasyon malzemeleriyle korunmaktadır.	*f*	7	12	39	102	39
		%	3,5	6,0	19,6	51,3	19,6
58	Doğal afetler, kötü niyetli saldırılar ve kazaklara karşı fiziksel koruma önlemleri büyük oranda alınmakta ve personel bilgilendirilmektedir.	*f*	9	27	52	103	8
		%	4,5	13,6	26,1	51,8	4,0
59	Elektrik, su, gaz ve diğer tedarik alt yapı hizmetlerini kesmek için acil durum anahtarları kullanılmaktadır.	*f*	10	19	40	76	54
		%	5,0	9,5	20,1	38,2	27,1

Tablo 6'daki veriler incelendiğinde, üniversite kütüphanelerindeki fiziksel ce çevresel varlıklarının güvenliğine ilişkin önlemelerden "kütüphanenin ana giriş ve çıkış kapılarının güvenlik birimi personeli ya da akıllı kapı sistemleri ile denetlenmesi (%77,4)", "kütüphanenin iç ve dış alanlarının güvenlik kameraları ile takip edilmesi (%70,9)", kritik bilgi

barındıran alanların fiziksel güvenlik sınırlarının güvenlik mekanizmaları ile korunması(%63,3), ve "kritik bilgilerin işlendiği veya saklandığı alanlara erişimin yetkili kişiler ile sınırlandırılması (%60,3)" konularındaki önlemlerin daha iyi düzeylerde uygulandığı belirlenmiştir.

Bu kategori altında, "refakat edilmeyen ziyaretçilere yaka kısımlarında görünür şekilde ziyaretçi kartı takma zorunluluğunun uygulanması" önlemi, en az oranda (%26,6) iyi düzeyde uygulanan önlem olarak belirlenmiştir. Ayrıca, bu önlemin hiç uygulanmama oranı (%34,2) ile en yüksek orana sahip olduğu tespit edilmiştir.Ayrıca bu kategoride yer alan önlemlerin hiç uygulanmadığına ilişkin katılımcı görüşlerinin diğer kategorilerdeki önlemlerin uygulanma düzeylerine göre daha yüksek oranlarda (%3,5 ile %34,2 arasında) olduğu tespit edilmiştir. Bu duruma en büyük etmenin katılımcıların bilgi güvenliği yönetimi ile ilgili fiziksel ve çevresel önlemler hakkında daha çok bilgi sahibi olmaları veya bu konuda kütüphane yönetimlerinin daha iyi düzeylerde bilgilendirme faaliyetlerini gerçekleştirdikleri söylenebilir. Bu kategori altında yer alan önlemelerin üniversite kütüphanelerinde uygulanmalarına ilişkin katılımcıların fikir sahibi olmama oranının diğer teknolojik kategorilerdeki önlemlere göre çok düşük olması bu durumu kanıtlar niteliktedir. Sadece 57. (%19,6) ve 59. maddelerdeki (%27,1) önlemlere ilişkin katılımcıların fikir sahibi olmama oranın yüksek olması, bu tür önlemlerin kütüphane dışı teknik birimler tarafından takip edilmesi ve kütüphane personelinin bu konularda bu birimlerce bilgilendirilmemesine bağlanabilir.

Kurumsal Bilgi Güvenliği Önlemelerinin Uygulanma Düzeyleri

Bu başlık altında, üniversite kütüphanelerinde kurumsal bilgi güvenliği önlemlerinden bilgi güvenliği politikaları (Tablo 7), bilgi güvenliği prosedürleri (Tablo 8), bilgi güvenliği idari araç ve yöntemleri (Tablo 9) ve bilgi güvenliği farkındalık çalışmaları (Tablo 10) kategorilerde yer alan önlem maddelerinin uygulama düzeyleri hakkında katılımcıların görüşlerine ilişkin frekans dağılımları verilmiştir.

Tablo 7: Bilgi güvenliği politikalarının uygulanma düzeyleri

	Bilgi Güvenliği Politikaları Maddeleri		*Uygulanma Düzeyi*				*Fikrim yok*
			Hiç	*Kötü*	*Orta*	*İyi*	
1	Personel, kullanıcı ve tedarikçilerin bilgi sistemleri ve varlıklarındaki bilgilerin kabul edilebilir kullanımlarını tanımlayan ilkeler	*f*	8	13	53	102	23
		%	4,0	6,5	26,6	51,3	11,6
2	Kâğıt veya elektronik ortamda bulunan kritik bilgilere yetkisiz erişim, bunların hasar görmesi ve kaybolması risklerini azaltan temiz masa / ekran ilke ve yöntemleri	*f*	10	11	49	98	31
		%	5,0	5,5	24,6	49,2	15,6
3	Kritik bilgi, evrak, yazılım ve diğer bilgi varlıklarının kurum dışına çıkarılması ya da başka ortamlara aktarılması ile ilgili bilgi transferi ilke ve yöntemleri	*f*	10	15	39	107	28
		%	5,0	7,5	19,6	53,8	14,1
4	Taşınabilir cihazların kullanılmasıyla ortaya çıkan risklerin yönetilmesini ve üzerlerindeki kayıtlı bilgilerin güvenliğini temin eden ilkeler	*f*	10	17	48	94	30
		%	5,0	8,5	24,1	47,2	15,1
5	Uzak çalışma alanlarından kurumun bilgi sistemlerinde işlenen ve depolanan bilgiyi koruma amacı güden uzaktan çalışma ilkeler	*f*	6	11	49	106	27
		%	3,0	5,5	24,6	53,3	13,6
6	Bilgi sistemlerine kaynağı belirli, kişisel ve kötü niyet şüphesi olmayan hangi tür yazılımların kurulabileceğini tanımlayan ilke ve yöntemler	*f*	9	13	41	97	39
		%	4,5	6,5	20,6	48,7	19,6
7	Bilgi sistemleri ve varlıklarına erişim sağlayan kullanıcı ve tedarikçilerin haklarını, kısıtlamalarını ve sınırlığını belirleyen erişim kontrol ilke ve yöntemleri	*f*	8	14	41	110	26
		%	4,0	7,0	20,6	55,3	13,1
8	Bilginin değeri, kritikliği ve ifşa edilme hassasiyetine uygun seviyelerde korunmasını teminen bilgi sınıflandırma ve etiketleme ilkeleri	*f*	8	18	44	101	28
		%	4,0	9,0	22,1	50,8	14,1
9	Kritik bilgi barındıran alan ve sistemlerin korunmasını ve kütüphanenin güvenlik sınırlarını ve önlemlerini tanımlayan fiziksel ve çevresel güvenlik ilke ve yöntemleri	*f*	9	21	49	100	20
		%	4,5	10,6	24,6	50,3	10,1
10	Olası bir felaket ve ortam hatasından kaynaklanan veri kaybına karşı kritik bilgi, yazılım ve sistemlerin korunmasını amaçlayan bilgi yedekleme ilke ve yöntemleri	*f*	10	10	38	111	30
		%	5,0	5,0	19,1	55,8	15,1
11	Bilgi sistemlerinin zararlı yazılım saldırılarından korumak için tespit etme, engelleme ve kurtarma kontrollerini içeren zararlı yazılımlara karşı ilke ve yöntemler	*f*	9	7	43	109	31
		%	4,5	3,5	21,6	54,8	15,6
12	Bilgilerin gizliliğinin ve bütünlüğünün korunması için şifreleme kontrollerinin doğru ve etkin kullanımını temin eden ilke ve yöntemler	*f*	8	9	44	110	28
		%	4,0	4,5	22,1	55,3	14,1
13	Ağa bağlı sistem ve uygulamalardaki verilerin ve ağ alt yapısının güvenliğini ve yetkisiz erişimlerden korunmasını temin eden ağ yönetimi ilke ve yöntemleri	*f*	8	7	37	113	34
		%	4,0	3,5	18,6	56,8	17,1
14	Kişisel kimlik bilgilerinin gizliliğini ve korunmasını temin eden kişisel bilgilerin mahremiyeti ve koruması ilke ve yöntemleri	*f*	8	10	39	125	17
		%	4,0	5,0	19,6	62,8	8,5
15	Patentli yazılım ve bilgi varlıklarının yasal kullanım haklarının ilgili yasa ve anlaşmalar çerçevesinde korunmasını temin eden fikri mülkiyet ilke ve yöntemleri	*f*	8	7	39	112	33
		%	4,0	3,5	19,6	56,3	16,6
16	Tedarikçilerin kullanıcı ve kurumsal bilgi varlıklarına erişimi ile ilgili risklerin azaltılmasını ve kritik bilgilerin korunmasını temin eden tedarikçi ilişkileri yöntemleri	*f*	7	9	42	103	38
		%	3,5	4,5	21,1	51,8	19,1

Tablo 7'deki veriler incelendiğinde, üniversite kütüphanelerinde bilgi güvenliği politikalarına ilişkin uygulamaların takribi %50 oranlar ile iyi düzeylerde uygulandığı belirlenmiştir. Bilgi güvenliği politikalarının hiç olmadığına ilişkin görüşlerin en yüksek oranın %5,0 ile "olası bir felaket ve ortam hatasından kaynaklanan veri kaybına karşı kritik bilgi, yazılım ve sistemlerin korunmasını amaçlayan bilgi yedekleme ilke ve yöntemleri" uygulamasının olduğu görülmüştür. Fakat bu önlemlerin uygulanma düzeylerinin kurumsal bilgi güvenliği açısından yeterli düzeyde olmadığı söylenebilir.

Bilgi güvenliği politikalarına ilişkin fikri olmayan katılımcıların oranın ise %8,5 ile %19,6 oranları arasında olması ise düşündürücü düzeydedir.

Katılımcıların kurumsal güvenlik politikalarından haberdar olmaması, politikaların varlığına ilişkin kütüphane yönetimlerinin bilgilendirme eksikliklerinin olduğu veya bilgi güvenliği ile ilgili farkındalık çalışmalarının iyi düzeylerde yapılmadığı düşüncelerini ön plana çıkarmaktadır.

Tablo 8: Bilgi güvenliği prosedürlerinin uygulama düzeyleri

	Bilgi Güvenliği Prosedürleri		***Uygulanma Düzeyi***				***Fikrim yok***
			Hiç	***Kötü***	***Orta***	***İyi***	
17	Kritik bilgilerin yedeklendiği ve taşındığı ortamların güvenli bir biçimde kullanılması, taşınması ve imha edilmesi ile ilgili faaliyetleri düzenleyen ilke ve yöntemler	*f*	9	8	43	97	42
		%	4,5	4,0	21,6	48,7	21,1
18	Sistem ve hizmetlere güvenli erişimi temin etmek için kullanıcı kaydetme, kayıt silme, erişim izni verme, kimlik doğrulama gibi faaliyetlerin belirlendiği kullanıcı erişim ilke ve yöntemleri	*f*	9	5	38	121	26
		%	4,5	2,5	19,1	60,8	13,1
19	Sistem ve uygulamalara yetkisiz erişimi engellemek için faaliyetlerin belirlendiği güvenli oturum açma ilke ve yöntemleri	*f*	6	7	39	120	27
		%	3,0	3,5	19,6	60,3	13,6
20	Güvenli alanlara sadece yetkili personele erişim izni vermek için uygun giriş kontrollerinin ve faaliyetlerinin belirlendiği fiziksel giriş ilke ve yöntemleri	*f*	11	9	39	114	26
		%	5,5	4,5	19,6	57,3	13,1
21	Bilgi güvenliği ihlal olaylarına hızlı, etkili ve düzenli bir şekilde müdahale edilmesini amaçlayan faaliyetlerin ve yönetim sorumluluklarının belirlendiği ilke ve yöntemler	*f*	12	13	40	94	40
		%	6,0	6,5	20,1	47,2	20,1
22	Yıkıcı bir olayı yönetmek ve mevcut durumu korumak veya en az zararla atlatabilme için gereksinim duyulan planlama ve faaliyetlerin belirlendiği iş sürekliliği ve felaket kurtarma ilke ve yöntemleri	*f*	14	15	40	96	34
		%	7,0	7,5	20,1	48,2	17,1
23	Kütüphane sistemleri, internet ağı, elektronik posta ve diğer erişimler için güçlü parola kullanımı ve yönetme standartları düzenleyen parola işleme ve kullanımı ilke ve yöntemleri	*f*	7	9	39	120	24
		%	3,5	4,5	19,6	60,3	12,1
24	Bilgi varlıklarının kapasitelerinin planlanması ve kapasite kullanımlarının belli sınırlar içinde tutulması faaliyetlerini düzenleyen kapasite yönetimi ilke ve yöntemleri	*f*	12	6	45	105	31
		%	6,0	3,0	22,6	52,8	15,6
25	Kullanıcıların doğru ve güvenli e-posta kullanımına yönelik kişisel ve kurumsal faaliyetleri düzenleyen elektronik posta ilke ve yöntemleri	*f*	8	10	37	116	28
		%	4,0	5,0	18,6	58,3	14,1
26	Ziyaretçilerin kabulü, dolaşımları ve kütüphaneden ayrılmalarıyla ilgili faaliyetleri düzenleyen ziyaretçi kabul ilke ve yöntemleri	*f*	17	16	48	97	21
		%	8,5	8,0	24,1	48,7	10,6

Tablo 8'deki veriler incelendiğinde, üniversite kütüphanelerinde bilgi güvenliği prosedürlerine ilişkin uygulamaların politikalarda olduğu gibi iyi seviyelere yakın düzeylerde uygulandığı belirlenmiştir. Özellikle, sistem ve hizmetlere güvenli erişimi temin eden kullanıcı erişimine ilişkin ilke ve yöntemler (%60,8), sistem ve uygulamalara yetkisiz erişimi engellemek için faaliyetlerin belirlendiği güvenli oturum açma ilke ve yöntemleri (%60,3) ve güçlü parola kullanımı standartlarını düzenleyen parola işleme ve kullanımı ilke ve yöntemleri (%60,3) uygulamalarının diğer prosedür uygulamalarına göre daha iyi düzeylerde uygulandığı görülmüştür.

Bilgi güvenliği prosedürlerinin hiç uygulanmadığına ilişkin katılımcı görüşlerinin en yüksek oranının %8,5 olması, bu kategoride yer alan

uygulamaların bir üst kurumsal önlem basamağında yer alan kurumsal bilgi güvenliği politikalarına göre artmasının sebebi olarak prosedürlerin politikalara bağlı olarak yürütülmesi söylenebilir. Bu nedenle bilgi güvenliği prosedürlerinin politikalara göre daha iyi uygulanamaması kütüphane yönetimlerinin kurumsal güvenlik araçlarını iyi seviyelerde planlayamadıkları görüşünü öncelikli olarak düşündürmektedir. Bilgi güvenliği prosedürlerinin varlığına ilişkin fikri olmayan katılımcıların %10,6 ile %21,1 oranları arasında olması da bu düşünceyi desteklemektedir. Çünkü bilgi güvenliği politikalarının iyi bir biçimde planlanmaması ve uygulanmaması bilgi güvenliği prosedürlerinin de iyi düzeylerde uygulanamamasına ve bu konuda daha çok bilgi eksikliklerinin oluşmasına neden olduğu anlaşılmaktadır.

Tablo 9: Bilgi güvenliği idari araç ve yöntemlerinin uygulama düzeyleri

	Bilgi Güvenliği İdari Araç ve Yöntemleri Maddeleri		***Uygulanma Düzeyi***				***Fikrim yok***
			Hiç	***Kötü***	***Orta***	***İyi***	
27	Bilgi güvenliği politika ve prosedürleri ihlallerinin raporlanması ve ilgili birimlere bildirilmesini düzenleyen kılavuz ve talimatlar	*f*	18	19	46	86	30
		%	9,0	9,5	23,1	43,2	15,1
28	Bilgi güvenliği ihlal olayını gerçekleştiren çalışanlara yönelik önlem almak için resmi bir disiplin mekanizması	*f*	12	16	41	87	43
		%	6,0	8,0	20,6	43,7	21,6
29	Yeni istihdam edilen personele bilgi güvenliği sorumluluklarını ve görevi son bulan personele ise istihdamın sona ermesinden sonra devam ettirmesi gereken bilgi güvenliği sorumluluklarını bildiren talimat ve uygulamalar	*f*	16	22	46	89	26
		%	8,0	11,1	23,1	44,7	13,1
30	Kişisel bilgilerin kütüphane bilgi sistemlerine işlenmeden önce ilgili kullanıcının bilgilendirilmesini amaçlayan aydınlatma metni uygulamaları	*f*	14	12	47	102	24
		%	7,0	6,0	23,6	51,3	12,1
31	Kişisel bilgilerin kütüphane bilgi sistemlerine işlenme amacının ilgilisine açıkça ifade edilmesini amaçlayan açık rıza yönetimi uygulamaları	*f*	17	12	47	99	24
		%	8,5	6,0	23,6	49,7	12,1
32	Bilgi güvenliği tehditlerinden korumaya yönelik ilgili aksiyon planlarını kapsayan risk analizi tabanlı idari araçlar ve uygulamalar (varlık performans analizi, tehdit analizi, risk analizi vb.)	*f*	12	15	41	87	44
		%	6,0	7,5	20,6	43,7	22,1
33	Bilgi güvenliği yönetim sisteminin etkin, güncel, izlenebilir ve gelişime açık yapıda olmasını amaçlayan iç denetim ilke ve uygulamaları	*f*	10	14	42	98	35
		%	5,0	7,0	21,1	49,2	17,6
34	Üçüncü taraf tedarikçi firma ve kurumlar ile yapılacak bilgi alışverişinin güvenliğini sağlamaya yönelik yapılan sözleşmelere ilişkin idari ilke ve yöntemler	*f*	8	9	38	104	40
		%	4,0	4,5	19,1	52,3	20,1

Tablo 9'daki veriler incelendiğinde, üniversite kütüphanelerinde bilgi güvenliği idari araç ve yöntemlerine ilişkin uygulamalarının genel olarak %50 ve altı oranlarda iyi düzeylerde uygulandığı fakat bu düzeylerinde de yeterli düzeylerde olmadığı görülmüştür. Bu kategoride yer alan önlemlerin uygulanmasında katılımcıların kötü ve orta düzeyde de belirgin oranlarda görüş bildirdiği belirlenmiştir. Özellikle %12,1 ile %22,1 oranları arasında katılımcının bilgi güvenliği idari araç ve yöntemlerinin varlığına ilişkin fikrinin olmaması, bu kategorideki uygulama düzeylerinin daha üst kurumsal

önlem basamaklarında yer alan politika ve prosedürlere göre düşük oranlarda uygulanmasını destekler niteliktedir.

Kurumsal bilgi güvenliği önlenmeleri bir bütün olarak düşünüldüğünde idari araç ve yöntemlerinin politika ve prosedürlerden sonra önemli kurumsal araçlar olduğu fakat üniversite kütüphanelerinde bu önlemlere ilişkin üst seviyelerde uygulamaların olmadığı düşüncesini kuvvetlendirmektedir.

Tablo 10: Bilgi güvenliği farkındalık çalışmalarının uygulama düzeyleri

	Bilgi Güvenliği Farkındalık Çalışmaları		***Uygulanma Düzeyi***				***Fikrim yok***
			Hiç	***Kötü***	***Orta***	***İyi***	
35	Personelin ve kullanıcıların bilgi güvenliği sorumluluklarını farkında olmalarını ve yerine getirmelerini amaçlayan bilgi güvenliği farkındalık eğitimi çalışmaları	*f*	21	26	54	86	12
		%	10,6	13,1	27,1	43,2	6,0
36	Bilgi güvenliği eğitim faaliyetlerinin kapsamının belirlendiği ve ihtiyaçların netleştirildiği eğitim planlama rehberleri	*f*	27	30	52	74	16
		%	13,6	15,1	26,1	37,2	8,0
37	Bilgi güvenliği alanında görevlendirilen personelin yetenek ihtiyaç analizinin yapılması ve sonuçlarına göre hizmetçi eğitim uygulamaları	*f*	26	28	50	75	20
		%	13,1	14,1	25,1	37,7	10,1
38	Kütüphanenin bilgi güvenliği çerçevesini oluşturan politika, prosedür ve idari yöntemler hakkında tedarikçilerin farkındalığını geliştirme çalışmaları	*f*	26	22	51	79	21
		%	13,1	11,1	25,6	39,7	10,6
39	Personel ve kullanıcıların bilgi güvenliği farkındalığını arttırıcı interaktif eğitim çalışmaları	*f*	32	25	52	77	13
		%	16,1	12,6	26,1	38,7	6,5
40	Bilgi güvenliği ile ilgili broşür, poster ve kitapçık gibi bilgilendirici doküman çalışmaları	*f*	39	31	52	63	14
		%	19,6	15,6	26,1	31,7	7,0
41	Kütüphane içerisinde dijital ortamlardan bilgi güvenliği farkındalık düzeyini arttırmaya yönelik film gibi görsellerin sunulması	*f*	47	36	48	55	13
		%	23,6	18,1	24,1	27,6	6,5
42	Kütüphane bilgisayarlarında bilgi güvenliğini hatırlatıcı oturum açma mesajları, fare altlığı, not kâğıtları gibi farkındalık arttırıcı faaliyetler	*f*	42	38	47	60	12
		%	21,1	19,1	23,6	30,2	6,0
43	Personele ve kullanıcılara bilgi güvenliği ile ilgili mail ve SMS yoluyla bilgilendirme mesajlarının gönderilmesi	*f*	28	28	52	78	19
		%	14,1	14,1	26,1	39,2	6,5
44	Personel ve kullanıcıların bilgi güvenliği hassasiyetlerinin ödüllendirilme çalışmaları	*f*	55	36	42	45	21
		%	27,6	18,1	21,1	22,6	10,6
45	Kütüphanenizin bilgi güvenliği politika, prosedür ve idari yöntemleri ile ilgili yapılan güncellemelerin kullanıcılara zamanında bildirilme	*f*	27	24	49	84	15
		%	13,6	12,1	24,2	42,2	7,5

Tablo 10'daki veriler incelendiğinde, üniversite kütüphanelerinde bilgi güvenliği farkındalık çalışmalarına ilişkin uygulamaların düşük düzeylerde gerçekleştiği görülmüştür. Özellikle "personel ve kullanıcıların bilgi güvenliği hassasiyetlerinin ödüllendirilme çalışmaları (%27,6)" ve "kütüphane içerisinde dijital ortamlardan bilgi güvenliği farkındalık düzeyini arttırmaya yönelik film gibi görsellerin sunulması (%23,6)" ve "kütüphane bilgisayarlarında bilgi güvenliğini hatırlatıcı farkındalık arttırıcı faaliyetlerin düzenlenmemesi (%21,1)" bilgi güvenliği farkındalık faaliyetlerinin hiç uygulanmama oranlarının yüksekliği göze çarpmaktadır. Bu durum üniversite

kütüphanelerinin bilgi güvenliği farkındalık çalışmalarından yoksun olduğunu göstermektedir.

Bu kategoride yer alan uygulamalara ilişkin katılımcıların "hiç uygulanmakta" görüşü diğer kurumsal güvenlik kategorilerindeki uygulamalara göre daha üst seviyelerde olduğu hatta teknolojik güvenlik önlemlerine göre de daha yüksek olduğu görülmüştür. Bu durum üniversite kütüphanelerinde bilgi güvenliği farkındalık çalışmalarının hiç yapılmadığına ilişkin çıkarımları ön plana çıkarmaktadır. Ayrıca üniversite kütüphanelerinde bilgi güvenliği farkındalık çalışmaları yapılsa da bu uygulamalara ilişkin katılımcı görüşlerinin çoğunluğunun "kötü" ve "orta" düzeylerde olması, teknolojik ve kurumsal bilgi güvenliği önlem ve uygulamalarının yeterli düzeylerde olmamasını desteklemektedir.

Sonuç ve Öneriler

Bilgi güvenliği, hassas ve değerli bilgilerin yetkisiz erişim, değişiklik, ifşa veya yok edilme gibi olumsuz etkilerden korunmasını sağlayan bir dizi önlem ve uygulamaları içeren güvenlik alanıdır. Elektronik veya basılı ortamlardaki bilgilerin veya verilerin saklanması ve iletilmesi sırasında izinsiz erişim gibi oluşabilecek risklere karşı alınan veya alınacak önlemleri ve tedbirleri kapsamaktadır. Bilgi güvenliği, bilginin gizlilik, bütünlük ve erişilebilirlik unsurlarını koruyarak bilgi varlıklarının güvenliğini sağlamayı hedeflemektedir. Bunun için iyi bir bilgi güvenliği yönetim sistemine sahip olunması gerekir. Bilgi güvenliği yönetim sistemi, bir organizasyonun bilgi varlıklarını korumak için gerekli süreçleri ve politikaları içeren bir çerçeve yapıdır. Bu sistemin amacı, bilgi varlıklarının gizliliğini, bütünlüğünü ve erişilebilirliğini sağlamak ve organizasyonun kurumsal ve kişisel tüm bilgilerinin güvenliğini sağlayarak hizmetlerin sürekliliğini temin etmektir.

Üniversite kütüphaneleri, bilimsel bilgiye erişim merkezlerinden biridir. Öğrenciler, akademisyenler ve araştırmacılar için zengin bilgi kaynağı sunmaktadırlar. Dijital dönüşümün hız kazandığı günümüzde, bu kütüphanelerdeki bilgilerin güvenliği büyük önem taşımaktadır. Bu nedenle kütüphane bilgi sistemlerinde işlenen ve depolanan kurumsal ve kişisel bilgilerin korunması ve veri bütünlüğünün sağlaması için otoriter kurumlarca önerilen ya da yasal uygulamalar ile belirlenen standartlara uygun bilgi güvenliği önlem ve uygulamalarının geliştirilmesi ve uygulanması gerekir. Üniversite kütüphanelerinde iyi bir bilgi güvenliği yönetim anlayışı, akademik araştırmaların doğruluğunu ve güvenilirliğini sağlamak için kritik bir faktördür. Bu bağlamda üniversite kütüphaneleri, kullanıcılarına güvenli bir ortam sunmalı, veri güvenliği konusunda gerekli önlemleri almalı ve bilgi güvenliği politikalarını etkin bir şekilde uygulamalıdır. Bu itibarla Türkiye'de üniversite kütüphanelerinde teknolojik ve kurumsal bilgi güvenliği önlem ve uygulamalarının uygulanma düzeylerinin belirlenmesi amaçlanan bu

çalışmanın sonuçları ile kütüphanecilik alanında bu konuya ilişkin önemli katkılarda bulunulması düşünülmektedir.

Çalışmadan elde edilen bulgular, Türkiye'de üniversite kütüphanelerinde teknolojik ve kurumsal bilgi güvenliği önlemlerinin genel itibarıyla orta düzeylerde uygulandığı sonucuna ulaşılmıştır. Özellikle teknolojik bilgi güvenliği önlemlerinin (donanım, yazılım, ağ, veri, fiziksel ve çevresel) kurumsal bilgi güvenliği önlemlerine (politikalar, prosedürler, idari araçlar ve farkındalık çalışmaları) göre daha iyi düzeylerde uygulandığı tespit edilmiştir. Teknolojik güvenlik önlemlerinden donanım, yazılım, ağ ve veri güvenliği ile kurumsal güvenlik uygulamalarından politika, prosedür ve idari araçlar kategorilerinde yer alan önlem ve uygulamaların çoğunluğunun orta düzeyin üzerinde uygulandığı görülse de, bu bilgi güvenliği önlem ve uygulamalarına ilişkin daha fazla iyileştirmeye ihtiyacın olduğunu görülmektedir. Teknolojik güvenlik önlemlerinden fiziksel ve çevresel güvenlik önlemleri ile kurumsal güvenlik uygulamalarından farkındalık çalışmalarının ise düşük düzeylerde uygulandığı hatta hiç uygulanamadığı ile ilgili katılımcı görüşlerinin daha yüksek oranlarda olduğu görülmüştür. Bu bulgular, Türkiye'de üniversite kütüphanelerinde teknolojik ve kurumsal güvenlik önlem ve uygulamalarının genel itibarıyla takip edildiğini ancak yeterli düzeylerde uygulanmadığı sonucuna ulaştırmaktadır. Bu alanlardaki bazı önlem ve uygulamaların ise düşük seviyede uygulanmasının ise potansiyel güvenlik tehditlerinin artmasına ve bilgilerin gizliliği, bütünlüğü ve erişilebilirliği açısından risk oluşturmasına neden olabileceği sonucunu ortaya koymaktadır. Kurumsal bilgi güvenliği önlemleri içerisinde değerlendirilen bilgi güvenliği farkındalık çalışmalarına ilişkin uygulamaların diğer kategorilerdeki önlem ve uygulamalara göre en düşük düzeyde uygulanmasının ise Türkiye'de üniversite kütüphanelerinde iyi bir bilgi güvenliği yönetim sisteminin gelişmediğini göstermektedir.

Bilgi güvenliği farkındalık çalışmalarının düşük düzeylerde uygulanması hatta hiç uygulanmamasına ilişkin katılımcı oranların yüksek olması, diğer tüm kategorilerde yer alan önlem ve uygulamaların uygulanması konusunda katılımcıların herhangi bir bilgiye sahip olmama durumlarına yansıdığı görülmüştür. Özellikle dananım, yazılım, ağ, veri güvenliği önlemleri ile bilgi güvenliği politikaları, prosedürleri ve idari araçları kategorilerinde değerlendirilen bilgi güvenliği önlem ve uygulamaları konusunda katılımcıların "fikrim yok" görüşünün yoğun olduğu görülmüştür. Fiziksel ve çevresel güvenlik önlemlerinde ise "fikrim yok" seçeneğinin daha az oranlarda olduğu görülmüştür. Bu nedenle üniversite kütüphanelerinde bilgi güvenliği önlem ve uygulamalarının daha çok fiziksel ve çevresel güvenlik boyutu üzerinde durulduğunu ve bunun da yeterli düzeylerde yürütülmediğini göstermektedir. Bu durum Türkiye'de üniversite kütüphanelerinde bilgi güvenliği önlem uygulamalarına ilişkin bütünsel bir yaklaşımın gelişmediğini belirlemektedir.

Üniversite kütüphanelerinde yeterli düzeyde uygulanmayan bilgi güvenliği önlem ve uygulamaları, bilgi varlıklarında bulunan bilgileri çeşitli tehlikeler maruz bırakabilir. Bilgi varlıklarında depolanan hassas bilgiler, öğrenci ve araştırmacıların kişisel verileri, telif haklarına tabi yayınlar ve diğer değerli bilgilerin yetkisiz kişilerin eline geçmesi, akademik etiği üniversite kütüphanelerinin güvenilirliği ve itibarı tehlikeye atacak ciddi sonuçlar doğurabilir. Bu nedenle üniversite kütüphanelerinin kurumsal ve teknolojik bilgi güvenliği önlem ve uygulamalarını güçlendirmesi, aksaklıkları ve eksiklikleri iyileştirmesi için şu hususları dikkate alınması önerilmektedir:

- Kurum içinde bilgi güvenliği konusunda farkındalığı artırmak için düzenli olarak çalışanlara eğitimler verilmelidir. Bu eğitimler, bilgi güvenliği politikaları, prosedürleri, güvenli kullanım yönergeleri, veri koruma yöntemleri, güvenli internet kullanımı farkındalık konularını ve en iyi uygulamaları kapsamalıdır. Bilinçlendirme kampanyaları ve seminerler gibi etkinlikler de düzenlenmelidir. Personelin bilgi güvenliği konusunda bilinçli olması, güvenlik açıklarının ve hataların azaltılmasına yardımcı olacaktır.
- Güncel ve kapsamlı bilgi güvenliği politikaları oluşturulmalı ve tüm çalışanlar anlaşılır şekilde bilgilendirilmelidir. Bu politikalar, erişim kontrolleri, şifreleme, veri yedekleme, kullanıcı hesap yönetimi gibi teknolojik ve kurumsal bilgi güvenliği önlemlerine ilişkin konuları içermelidir. Bilgi güvenliği önlemlerini geliştirmek için dış kaynaklı hizmet sağlayıcılarını da değerlendirebilir. Bu sağlayıcılar, güvenlik denetimleri, saldırı tespiti ve engelleme, güvenlik olayı yönetimi gibi konularda uzmanlık sunabilirler.
- Donanım, yazılım, ağ ve veri güvenliği önlemleri güncel tutulmalı ve düzenli olarak güvenlik açıkları taraması ve güncelleme işlemleri yapılmalıdır. Güçlü parola politikaları ve çok faktörlü kimlik doğrulama gibi önlemler uygulanmalıdır. Kütüphane sistemlerinde güncel antivirüs yazılımları, güvenlik duvarları ve saldırı tespit sistemleri gibi güvenlik yazılımları kullanılmalıdır. Bu yazılımlar düzenli olarak güncellenmeli ve izlenmelidir.
- Kütüphane alanına erişimi kontrol etmek için fiziksel güvenlik önlemleri alınmalıdır. Bu önlemler arasında güvenlik kameraları, kapı erişim sistemleri, alarm sistemleri ve izinli personel dışında girişleri kısıtlayan kontroller yer alabilir. Hassas bilgilerin bulunduğu alanlara sınırlı erişim sağlanmalı ve fiziksel kaynaklara yetkisiz erişimi engellemek için gerekli kontroller yapılmalıdır.
- Hassas verilerin korunması için veri şifreleme yöntemleri ve veri yedekleme stratejileri kullanılmalıdır. Veri kaybını önlemek için düzenli yedeklemeler ve veri kurtarma testleri yapılmalıdır.

Sistemlerdeki kullanıcı faaliyetleri izlenmeli ve olağandışı etkinlikler veya güvenlik ihlalleri tespit edildiğinde derhal müdahale edilmelidir. Bu amaçla, güvenlik olaylarının izlenmesi ve logların düzenli olarak denetlenmesi gerekmektedir.

- Bilgi güvenliği açısından kritik olan süreçlerin iş sürekliliği planları oluşturulmalı ve felaket durumlarında verilerin ve hizmetlerin hızlı bir şekilde geri kazanılması için felaket kurtarma planları geliştirilmelidir. Olası olaylar (doğal afetler, sistem arızaları vb.) karşısında iş sürekliliği planlaması yapmalıdır. Bu planlar, veri yedeklemesi, acil durum iletişim planları ve hızlı bir şekilde normal faaliyete dönme stratejilerini içermelidir.
- Bilgi güvenliği önlemlerini sürekli olarak gözden geçirmek ve iyileştirmek önemlidir. Düzenli olarak risk değerlendirmeleri yapılmalı, güvenlik açıkları tespit edilmeli ve düzeltici önlemler alınmalıdır. Güvenlik olayları ve ihlalleri izlemek ve bunlara uygun şekilde yanıt vermek için güvenlik olayı yönetimi süreçleri oluşturulmalıdır. Ayrıca, kullanıcı geri bildirimleri ve deneyimlerden yararlanarak sürekli olarak bilgi güvenliği politikaları ve prosedürleri güncellenmelidir.
- Üniversite kütüphaneleri, diğer üniversiteler ve bilgi güvenliği uzmanlarıyla işbirliği yaparak en iyi uygulamaları ve güncel bilgi güvenliği trendlerini paylaşmalıdır. Bu işbirliği, sektör genelinde bilgi güvenliği standartlarının yükseltilmesine katkıda bulunabilir. Kütüphane yönetimi, iç kontrol mekanizmalarını etkin bir şekilde uygulamalı ve düzenli olarak denetimler yapmalıdır. Bu, bilgi güvenliği önlemlerinin etkinliğini değerlendirmek, hataları tespit etmek ve düzeltici önlemler almak için önemlidir.
- Bilgi güvenliği, gizlilik, bütünlük ve erişilebilirlik gibi önemli unsurları korumak için sürekli bir çaba gerektirir. Kurumsal farkındalık, eğitim, teknolojik önlemler, fiziksel güvenlik ve veri koruması gibi alanlarda yapılan iyileştirmeler, üniversite kütüphanelerinin bilgi güvenliği yönetiminde daha etkili olmalarını sağlayabilir.

Bu çalışmada, Türkiye'de üniversite kütüphanelerinde teknolojik ve kurumsal bilgi güvenliği önlemlerinin uygulanma düzeylerinin mevcut durumu tespit edilerek bu önlemlerin yeterliliği konusunda değerlendirmelerde bulunulmaya çalışılmıştır. Gelecekte yapılacak çalışmalarda diğer kütüphane türlerinin ve bilgi merkezlerinin bu konuda yapılacak çalışmalara dâhil edilmesi önerilmektedir. Böylelikle, kütüphanecilik alanında bilgi güvenliği konusuna ilişkin durum tespiti yapılarak kütüphanecilik hizmetlerindeki bilgi güvenliği faaliyetlerinin

gelişimine katkı sunulabilir. Ayrıca kütüphanecilik alanında gelecekte yapılacak çalışmalara ilişkin şu konularında değerlendirilmesi önerilmektedir:

- Üniversite kütüphanelerinde kullanılan bilgi güvenliği standartlarının belirlenmesi ve incelenmesi için araştırmalar yapılabilir. Bu çalışmalar, kütüphanelerin mevcut güvenlik uygulamalarını değerlendirmek ve daha iyi bir güvenlik çerçevesi oluşturmak için temel teşkil edebilir.
- Kütüphanelerin güvenlik düzeylerini değerlendiren ve mevcut önlemlerin etkinliğini analiz eden çalışmalar yapılabilir. Bu incelemeler, kütüphanelerdeki güvenlik açıklarını belirlemek, potansiyel tehditleri ortaya çıkarmak ve daha güvenli bir ortam oluşturmak için stratejik öneriler sunabilir.
- Kütüphane kullanıcılarının bilgi güvenliği farkındalığı ve eğitimi üzerine araştırmalar yapılarak, kullanıcı davranışlarını anlamak ve güvenlik bilincini artırmak için önemlidir. Bu çalışmalar, kullanıcıların güvenlik politikalarını ve önlemlerini ne kadar benimsediklerini, güvenlik konusunda ne kadar bilinçli olduklarını ve güvenlikle ilgili sorumluluklarını nasıl algıladıklarını inceleyebilir.
- Yeni teknolojilerin üniversite kütüphanelerindeki bilgi güvenliğine etkisi üzerine çalışmalar yapılabilir. Örneğin, yapay zekâ, blok zincir, büyük veri analitiği gibi teknolojik yeniliklerin kütüphanelerdeki güvenlik açıklarını kapatmada nasıl kullanılabileceği ve daha güçlü güvenlik çözümleri sunabileceği araştırılabilir.
- Üniversite kütüphanelerinin bilgi güvenliği konusunda işbirliği ve paylaşımın önemi üzerine çalışmalar yapılabilir. Bu çalışmalar, kütüphaneler arasında bilgi güvenliği en iyi uygulamalarının paylaşılmasını teşvik edebilir ve sektördeki diğer kurumların benzer sorunlarla nasıl başa çıktığını anlamak için önemli bir kaynak olabilir.
- Kütüphane kullanıcılarının sosyal mühendislik ve sosyal medya üzerine odaklanan tehditlerle nasıl etkileşimde bulunduğunu ve güvenlik açıklarının nasıl sömürüldüğünü inceleyen araştırmalar yapılabilir. Bu çalışmalar, kütüphane kullanıcılarının sosyal medya güvenliği konusunda farkındalığını artırabilir ve sosyal mühendislik saldırılarına karşı daha iyi savunma stratejileri geliştirmeye yardımcı olabilir.
- İnsan faktörünün bilgi güvenliği üzerindeki etkisini araştıran çalışmalar yapılarak kütüphane personelinin ve kullanıcıların bilgi güvenliği ile ilgili davranışları ve kararları analiz edebilir. Bu çalışmalar, insan faktörünün güvenlik açıklarının ortaya çıkmasında ve saldırılara karşı savunmasızlıkta oynadığı rolü anlamak için

önemlidir. Ayrıca, bu araştırmalar, kütüphane kullanıcılarının ve personelinin güvenlik konusunda daha bilinçli olmalarını sağlamak için eğitim ve farkındalık programları geliştirmeye yönelik stratejiler sunabilir.

- Bilgi güvenliği alanında yeni ve yenilikçi yaklaşımları araştıran çalışmalar yapılarak üniversite kütüphanelerinin güvenlik açıklarını azaltmak için yeni çözümler sunabilir. Örneğin, yapay zekâ ve makine öğrenimi gibi teknolojilerin güvenlik alanında nasıl kullanılabileceği ve kütüphanelerdeki güvenlik stratejilerini nasıl güçlendirebileceği üzerine araştırmalar yapılabilir.

Genel olarak, Türkiye'deki üniversite kütüphanelerinde bilgi güvenliği yönetimine daha fazla önem verilmesi ve güvenlik önlemlerinin etkin bir şekilde uygulanması gerektiği sonucuna ulaşılmıştır. Bu, üniversite kütüphanelerindeki bilgilerin gizliliği, bütünlüğü ve erişilebilirliği açısından önemlidir ve akademik araştırmaların doğruluğunu ve güvenilirliğini sağlamak için kritik bir faktördür. Üniversite kütüphanelerinin bu alanda daha ileri adımlar atması ve bilgi güvenliği yönetimine yönelik daha bütünsel bir yaklaşım benimsemesi gerektiği düşünülmektedir.

Kaynakça

Aksu, P. K. (2014). *Hastane bilgi yönetim sisteminin bilgi güvenliği açısından değerlendirilmesi* (Yayımlanmamış yüksek lisansdoktora tezi). Marmara Üniversitesi Sağlık Bilimleri Enstitüsü, İstanbul.

American Library Association [ALA]. (2006). Resolution on the retention of library usage records. 2006 ALA Annual Conference. Erişim adresi: https://alair.ala.org/handle/11213/1594

Amini, M., Vakilimofrad, H. ve Saberi, M. K. (2021). Human factors affecting information security in libraries. *The Bottom Line, 34*(1), 45-67. doi.org/10.1108/BL-04-2020-0029

Association of College and Research Libraries(ACRL). (2016). Framework for information literacy for higher education. Erişim adresi: http://www.ala.org/acrl/standards/ilframework

Başdinkçi, N. (2017). *Sağlık kurumlarında bilgi güvenliği risk değerlendirilmesi ve kullanıcıların bilgi güvenliği farkındalık düzeyinin ölçülmesi* (Yayımlanmamış yüksek lisans tezi). Çukurova Üniversitesi Fen Bilimleri Enstitüsü, Adana.YÖK Tez Kataloğu veri tabanından erişildi.

Büyüköztürk, Ş., Kılıç Çakmak, E., Akgün, Ö. E., Karadeniz, Ş., ve Demirel, F. (2022). *Bilimsel araştırma yöntemleri* (32. Baskı). Ankara: Pegem Akademi Yayıncılık.

Çimen, Z.(2021). *Sağlık kurumlarında bilgi güvenliği ve çalışan görüşleri: Ankara ili özel hastane örneği* (Yayımlanmamış yüksek lisans tezi). Ankara Hacı Bayram Veli Üniversitesi Lisansüstü Eğitim Enstitüsü, Ankara. YÖK Tez Kataloğu veri tabanından erişildi. (Tez No: 706585)

Da Veiga, A. ve Eloff, J. H. P. (2010). A framework and assessment instrument for information security culture. *Computers & Security, 29(2),* 196-207. doi.org/10.1016/j.cose.2009.09.002

Dursun, İ. ve Alnıaçık, Ü. (2019). Likert ölçeklerinde seçenek etiketleme kararları: kullanılan etiketler ölçüm sonuçlarını etkiler mi?. *Journal of social sciences/sosyal bilimler dergisi, 33*. doi.org/10.14520/adyusbd.549447

Erol, S. E. (2016). *Siber güvenlik farkındalığı için yetenek tabanlı dinamik model* (Yayımlanmamış yüksek lisans tezi). Gazi Üniversitesi Fen Bilimleri Enstitüsü, Ankara.YÖK Tez Kataloğu veri tabanından erişildi. (Tez No: 449489)

Eşitti, B. (2018). Nicel araştırma yöntemleri: SPSS uygulamalı. D. A. Arslan (Ed), *Sosyal bilimlerde araştırma yöntem ve teknikleri* içinde (s.307-340). Çanakkale: Paradigma Akademi Yayınları

Evrin, V. ve Demirer, M. (2011). Kurumsal bilgi güvenliği süreç çalışmaları: ISO/IEC-27001 örneği. *IV. Ağ ve bilgi güvenliği sempozyumu el kitabı* (ss. 25-30). İçinde. Ankara: TMMOB Elektrik Mühendisleri Odası Yayınları.

Filik, T. (2020). *Tıbbi sekreterlerde bilgi güvenliği farkındalık düzeyinin elektronik sağlık kayıtlarının güvenlik ve mahremiyet uygulamalarına etkisinin değerlendirilmesi* (Yayımlanmamış yüksek lisans tezi). Kayseri Üniversitesi Lisansüstü Eğitim Enstitüsü, Kayseri.YÖK Tez Kataloğu veri tabanından erişildi.

Fox, E. ve ElSherbiny, N. (2011). Security and digital libraries. K. H. Huang (Ed.), *Digital Libraries-Methods and Applications* (s. 151-160). iİçinde. Published by im Tech

Fraenkel, J. R. and Wallen, N. E. (2006). *How to desing and evaluate research in education*. New York: McGaw-Hill

Gillaspy, M. L. (2005). Factors affecting the provision of consumer health ınformation in public libraries: The last five years. Mays, Tammy L. (Eds.). *Introduction to Library Trends 53 (3) Winter 2005: Consumer Health Issues, Trends, and Research, Part 2: Applicable Research in*

the 21st Century (s. 480-495) içinde. (s. 480-495) Illinois library. Erişim adresi: https://www.ideals.illinois.edu/handle/2142/1738

Güler, C. ve Furat, F. (2022). Belge yönetimi ve arşiv uygulamalarının bilgi güvenliği ilkelerine katkısı: Kavramsal bir değerlendirme. *Türk Kütüphaneciliği, 36*(1), 74-89. doi.org/10.24146/tk.1012325

Gülseçen, S. (2012). *Bilgi ve bilginin yönetimi.* İstanbul: Papatya Yayıncılık.

Güngör, M. (2015). *Ulusal bilgi güvenliği: Strateji ve kurumsal yapılanma*. (Uzmanlık tezi). Erişim adresi: http://www.bilgitoplumu.gov.tr/

Güriş, S. ve Astar, M. (2014). *Bilimsel araştırmalarda SPSS ile istatistik.* İstanbul: Der yayınları.

Gürsel, T. (2019). *Sigorta şirketlerinde bilgi güvenliği yönetim sistemi denetimi* (Yayımlanmamış yüksek lisans tezi). Marmara Üniversitesi Bankacılık ve Sigortacılık Enstitüsü, İstanbul.YÖK Tez Kataloğu veri tabanından erişildi.

Güvenlik. (t.y.). *Türk Dil Kurumu güncel Türkçe sözlük* içinde. Erişim adresi: https://sozluk.gov.tr/

Henkoğlu, T. (2015). *Hassas bilgi varlıklarının ve kişisel verilerin hukuksal düzenlemeler ile korunması ve bu kapsamda üniversiteler için bilgi güvenliği politikasının geliştirilmesi* (Yüksek lisansYayımlanmamış doktora tezi). Hacettepe Üniversitesi Sosyal Bilimler Enstitüsü, Ankara.YÖK Tez Kataloğu veri tabanından erişildi.

Henkoğlu, T. ve Uçak, N. Ö. (2015). Üniversite kütüphanelerinde kişisel verilerin korunması. *Bilgi Dünyası, 16*(1), 45-74. doi.org/10.15612/BD.2015.472

IFLA ve Kuhlenkamp, H. (2015*). IFLA iInternet mManifest 2014*. IFLA publications. Erişim adresi: https://repository.ifla.org/handle/123456789/1639

IFLA. (2012). *IFLA code of ethics for librarians and other ınformation workers*. International Federation of Library Associations. Erişim adresi: https://www.ifla.org/publications/ifla-statement-on-privacy-in-the-library-environment

IFLA. (2015). *IFLA statement on privacy in the library environment*. International Federation of Library Associations. Erişim adresi: https://www.ifla.org/publications/ifla-statement-on-privacy-in-the-library-environment/

Ismail, R. (2012). *Assessing information security management in Malaysian academic libraries* ([Doctoral dissertation), University of Malaya]. The

Universiti Malaya Research Repository. Erişim adresi: http://studentsrepo.um.edu.my/5537/

Kara, M. (2018). *Kurumsal Bilgi Güvenliği: Teknik ve Yönetimsel Yönleriyle*. İstanbul: Papatya Yayıncılık

Karasar, N. (2019).*Bilimsel araştırma yöntemi: Kavramlar ilkeler teknikler.* Ankara: Nobel Yayınları

Kemiksiz, R. C. (2022) Kişisel veri güvenliği üzerine bir alan araştırması: dijital yerliler ve dijital göçmenlerin güvenlik algıları. *Maltepe Üniversitesi İletişim Fakültesi Dergisi*, *9*(1), 64-91. Erişim adresi: https://dergipark.org.tr/en/pub/iled/issue/71183/1111856

Krosnick, J. A. ve Fabrigar, L. R. (1997). Designing rating scales for effective measurement in surveys. L. Lyberg ve diğerleri (Ed.), *Survey Measurement and Process Quality* i(s. 141-164). İçinde. Wiley-Interscience. doi.org/10.1002/9781118490013.ch6

Kurt, H. Ö. (2019). *Kurumlarda bilgi güvenliği yönetimi: Hastane bilgi sistemleri üzerine bir araştırma* (Yayımlanmamış yüksek lisans tezi). Necmettin Erbakan Üniversitesi Sağlık Bilimleri Enstitüsü, Konya.YÖK Tez Kataloğu veri tabanından erişildi. (Tez No: 557979)

Kurt, S. G. (2019). *Bilgi güvenliğinin bilgi işlem çalışanları tarafından değerlendirilmesi – Sağlık sektöründe bir çalışma* (Yayımlanmamış yüksek lisans tezi). Marmara Üniversitesi Sağlık Bilimleri Enstitüsü, İstanbul.YÖK Tez Kataloğu veri tabanından erişildi. (Tez No: 566816)

Marttin, V. ve Pehlivan, İ. (2010). ISO 27001:2005 Bilgi güvenliği yönetimi standardı ve Türkiye'deki bazı kamu kuruluşu uygulamaları üzerine bir inceleme. *Mühendislik Bilimleri ve Tasarım Dergisi, 1 (1)*, 49-56. Erişim adresi: https://dergipark.org.tr/en/pub/jesd/issue/20866/223911

Öztemiz, S. ve Yılmaz, B. (2013). Bilgi merkezlerinde bilgi güvenliği farkındalığı: Ankara'daki üniversite kütüphaneleri örneği. *Bilgi Dünyası, 14*(1), 87-100. doi.org/10.15612/BD.2013.136

Pathari, V. ve Sonar, R. (2012). Identifying linkages between statements in information security policy, procedures and controls. *Information Management & Computer Security*, *20(4)*, 264-280. doi.org/10.1108/09685221211267648

Peltier, T. R. (2016). *Information security policies, procedures, and standards: guidelines for effective information security management*. Boca Raton: CRC press.

Polat, C. (2006). Bilgi çağında üniversite eğitimi için bir açılım: bilgi okuryazarlığı öğretimi . *Atatürk Üniversitesi Türkiyat Araştırmaları Enstitüsü Dergisi , 12* (30) , 249-266. Erişim adresi: https://dergipark.org.tr/en/pub/ataunitaed/issue/2869/39227

Slade, R. (2006). *Dictionary of information security*. United Kingdom: Syngress Publishing.

Şahinaslan, E. (2010). *Standartlara dayalı bilgi güvenliği risk analiz ve ölçümleme metodolojisinin bankacılık sektörüne özgü modellenmesi ve uygulama yazılımının geliştirilmesi* (Yayımlanmamış Doktora üksek lisans tezi). Trakya Üniversitesi, Fen Bilimleri Enstitüsü, Edirne.YÖK Tez Kataloğu veri tabanından erişildi.

Şişkin, D. Ş.(2020). *Üniversite kütüphanelerinde bilgi güvenliği ve kişisel verilerin korunması: Ankara'daki üniversite kütüphanelerinin değerlendirilmesi* (Yayımlanmamış yüksek lisans tezi). Hacettepe Üniversitesi Sosyal Bilimler Enstitüsü, Ankrara.YÖK Tez Kataloğu veri tabanından erişildi. (Tez No: 620913)

Thomson, K. L., Von Solms, R. ve Louw, L. (2006). Cultivating an organizational information security culture. *Computer fraud & security*, *2006*(10), 7-11. doi.org/10.1016/S1361-3723(06)70430-4

Whitman, M. E. ve Mattord, H. J. (2011). *Roadmap to information security: For IT and infosec managers*. Boston: Cengage Learning.

Whitman, M. E. ve Mattord, H. J. (2018). *Principles of information security* (8nd ed.). Boston: Cengage Learning.

Workman, M., Bommer, W. H. ve Straub, D. (2008). Security lapses and the omission of information security measures: A threat control model and empirical test. *Computers in Human Behavior, 24*(6), 2799-2816. doi.org/10.1016/j.chb.2008.04.00

Yazıcıoğlu, Y. ve Erdoğan, S. (2014). *Bilimsel araştırma yöntemleri-SPSS uygulamalı* (4. baskı.). Ankara: Detay Yayıncılık.

Yükseköğretim Kurulu. [YÖK] (2022). *2022-2023 öğretim yılı yükseköğretim istatistikleri*. Yükseköğretim Bilgi Yönetim Sistemi, Yükseköğretim Kurulu. Erişim adresi: https://istatistik.yok.gov.tr/

Atıf için:

Kavak, A. ve Odabaş, H. (2023). Üniversite Kütüphanelerinde Teknolojik ve Kurumsal Bilgi Güvenliği Önlemlerinin Uygulanma Yeterliliği. *Çankırı Karatekin Üniversitesi Sosyal Bilimler Enstitüsü Dergisi*, 14(2), 293-332. doi: 10.54558/jiss.1321640

Etik Beyanı: Bu çalışmanın tüm hazırlanma süreçlerinde etik kurallara uyulduğunu yazarlar beyan eder. Aksi bir durumun tespiti halinde Çankırı Karatekin Üniversitesi Sosyal Bilimler Enstitüsü Dergisinin hiçbir sorumluluğu olmayıp, tüm sorumluluk çalışmanın yazarlarına aittir. Bu çalışma için etik kurul iznine gerek yoktur.

Yazar Katkıları: Yazarlar çalışmaya eşit oranda katkı sağlamıştır.

Çıkar Beyanı: Yazarlar arasında çıkar çatışması yoktur.