5. Uluslararası Gelenekten Geleceğe Bilgi ve Belge Yönetimi Sempozyumu
5-6 Kasım 2026, İstanbul

Ankara'da Bulunan Üniversite Kütüphanelerinin Bilgi Güvenliği Politikalarının İncelenmesi Üzerine Bir Çalışma

[1]Ankara'da Bulunan Üniversite Kütüphanelerinin Bilgi Güvenliği Politikalarının İncelenmesi Üzerine Bir Çalışma

Giriş

Kurumsal bilgi güvenliği politikaları, kurumların bilgi varlıklarını koruma, güvenlik risklerini en aza indirme ve yetkisiz erişimleri önleme amacıyla oluşturduğu stratejik belgelerdir. Bu politikalar yalnızca teknik tedbirleri içermekle kalmaz; aynı zamanda organizasyonel süreçleri, insan faktörünü ve yasal düzenlemeleri de kapsayan bütüncül bir güvenlik yaklaşımı sunmaktadır (ISO/IEC 27001, 2018; Von Solms ve Van Niekerk, 2013). Etkili bir bilgi güvenliği politikası, çalışanların sorumluluklarını ve güvenlik denetimlerini tanımlayarak, kurum genelinde bilgi güvenliği kültürünün oluşmasına katkı sağlamaktadır (Vural ve Sağıroğlu, 2008; Soliman ve Mohammadnazar, 2022). Bilgi güvenliği politikaları, teknik altyapının güçlendirilmesi, erişim yetkilerinin sınırlandırılması ve kullanıcı farkındalığının artırılması gibi uygulamalarla, kurumsal işleyişi destekleyen stratejik mekanizmalar oluşturur (ISO/IEC 27001, 2018; Cram ve diğerleri, 2017). Aynı zamanda, bilgi güvenliği farkındalığını teşvik ederek çalışanların rollerini tanımlar ve kurumsal sorumluluğu pekiştirir (Alhogail, 2015). Bu yönüyle bilgi güvenliği, yalnızca teknolojik önlemlere dayanmayan, insan faktörünü merkeze alan çok boyutlu bir yaklaşımdır (Gordon, Loeb ve Zhou, 2015). Bu çerçevede, bilgi güvenliği politika belgeleri, kurumun bilgi güvenliği stratejisini yansıtan, uygulanabilir ve sürdürülebilir önlemleri sistematik şekilde ifade eden resmi dokümanlardır (Karaarslan, 2003; Tekerek, 2008). Bu belgeler, bilgi güvenliği açıklarını azaltmakla kalmayıp; yasal düzenlemelere uyum, sürdürülebilir güvenlik yönetimi ve kurum itibarı açısından da kritik rol üstlenmektedir (Soomro, Shah ve Ahmed, 2016). Uygun şekilde yapılandırılmış ve kuruma özgü hazırlanmış politikalar, bilgi güvenliği alanında hem operasyonel başarı hem de kurumsal bütünlük açısından temel bir araç olarak değerlendirilmektedir.

Yöntem

Bu çalışma Ankara'daki üniversite kütüphanelerinde uygulanmakta olan bilgi güvenliği politikalarının tematik yapısını ortaya koymayı ve bilgi güvenliği politikalarını incelemeyi amaçlamaktadır. Çalışmada içerik analizi yöntemi kullanılmıştır. Çalışmaya Ankara'da bulunan toplam 14 üniversite dahil edilmiştir.

[1] Bu çalışma Ankara Yıldırım Beyazıt Üniversitesi Bilgi ve Belge Yönetimi Bölümünde yapılan üniversite kütüphanelerinde bilgi güvenliği politikalarının analizi ve kütüphanecilerin bilgi güvenliği farkındalık düzeylerinin belirlenmesi: Ankara'daki üniversite kütüphaneleri örneği başlıklı tezden üretilmiştir.

Bulgular

Üniversite kütüphanelerine ait politika belgelerinin amaçları incelendiğinde, üniversitelerin büyük çoğunluğunda gizlilik, bütünlük ve erişilebilirlik ilkelerinin temel bilgi güvenliği prensipleri olarak benimsendiği belirlenmiştir. Bununla birlikte bazı üniversitelerin politika belgelerinde risk yönetimi, iş sürekliliği, performansın izlenmesi ve ölçülmesi ile ISO/IEC 27001 standardına uyum gibi daha kapsamlı hedeflere de yer verildiği görülmektedir. Elde edilen bulgular, üniversitelerin temel bilgi güvenliği prensipleri bakımından büyük ölçüde ortak bir yaklaşım sergilemesine karşın, teknik ve operasyonel güvenlik uygulamalarında önemli farklılıklar ve eksiklikler bulunduğunu göstermektedir. İncelenen politika belgelerinin büyük bir bölümünde yedekleme süreçlerinin nasıl yürütüleceğini, sorumlulukları, yedekleme sıklığını ve olası veri kayıpları karşısında izlenecek süreci tanımlayan açık bir yedekleme planına yer verilmediği tespit edilmiştir.

Tartışma

Araştırma kapsamında incelenen bilgi güvenliği politika belgelerinde gizlilik, bütünlük ve erişilebilirlik ilkelerinin büyük ölçüde ortak bir çerçeve oluşturduğu; bunun yanı sıra teknik güvenlik uygulamalarının politika belgelerine aynı düzeyde yansımadığı belirlenmiştir. Bu bulgu, Kavak ve Odabaş'ın (2023) üniversite kütüphanelerinde kurumsal bilgi güvenliği yönetim araçlarının kullanımının teknolojik ve kurumsal güvenlik önlemlerinin uygulanma düzeyi üzerinde etkili olduğunu ortaya koyan sonuçlarıyla örtüşmektedir. Benzer şekilde Farid, Warraich ve Iftikhar (2023), akademik kütüphanelerde bilgi güvenliği politikalarının veri güvenliği, yedekleme, personel eğitimi, zararlı yazılımlar ve sosyal mühendislik gibi çok sayıda alanı birlikte kapsaması gerektiğini, ancak bu uygulamaların kütüphaneler arasında farklılık gösterdiğini belirtmektedir.

Sonuç

Sonuç olarak araştırma, üniversite kütüphanelerinin bilgi güvenliği politikalarında temel düzeyde kurumsal bir yapı oluşturduğunu; ancak teknik ve operasyonel güvenlik uygulamalarının politika belgelerine yeterince yansıtılamadığını ortaya koymaktadır. Özellikle yerli ve milli ürün kullanımı, veri şifreleme, sosyal mühendislik önlemleri, log yönetimi ve mobil cihaz güvenliği gibi kritik alanlardaki eksiklikler, üniversite kütüphanelerinin gelişen siber tehdit ortamı karşısında kırılganlığını artırmaktadır. Bu durum hem kurumsal bilgi varlıkları hem de kullanıcı verilerinin korunması için önemli bir yönetsel boşluğa işaret etmektedir.

Anahtar Kelimeler: Politika analizi, kütüphanelerde bilgi güvenliği, sosyal mühendislik

Kaynakça

Alhogail, A. (2015). Improving information security awareness in organizations: A study of critical success factors. Procedia Computer Science, 65, 1052–1058. https://doi.org/10.1016/j.procs.2015.09.072

Cram, ve diğerleri (2017). Kurumsal bilgi güvenliği politikaları: bir inceleme ve Araştırma çerçevesi. Avrupa Bilgi Sistemleri Dergisi, 26 (6), 605–641. https://doi.org/10.1057/s41303-017-0059-9

Ahmed Baki ŞAFAK ve Demet SOYLU

Öğretim Görevlisi, Ankara Üniversitesi, Yönetim ve Organizasyon Bölümü, ahmedbakisafak@gmail.com
Dr. Öğr. Üyesi, Ankara Yıldırım Beyazıt Üniversitesi, Bilgi ve Belge Yönetimi Bölümü, bunchnoble@gmail.com

Farid, G., Warraich, N. F., & Iftikhar, S. (2025). Digital information security management policy in academic libraries: A systematic review (2010–2022). *Journal of Information Science*, *51*(4), 1000-1014. https://doi.org/10.1177/01655515231160026

Gordon, L. A., Loeb, M. P., & Zhou, L. (2015). Investing in cybersecurity: Insights from the Gordon–Loeb model. Journal of Information Security, 6(2), 24–30. https://doi.org/10.4236/jis.2015.62003

ISO/IEC. (2013). ISO/IEC 27001 (2013). Information technology – Security techniques – Information security management systems Requirements. https://www.iso.org/obp/ui/#iso:std:iso-iec:27001:ed-2:v1:en.

Karaarslan E., ve diğerleri, (2003). Bilgisayar Ağlarında Güvenlik Politikalarının uygulanması. *Akademik Bilişim, Çukurova Üniversitesi*.

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. https://doi.org/10.54558/jiss.1321640

Soliman, W., ve Mohammadnazar, H. (2022). New Insights into the Justifiability of Organizational Information Security Policy Noncompliance : A Case Study. *In Proceedings of the 55th Hawaii International Conference on System Sciences (HICSS 2022)* 6812–6821. https://doi.org/10.24251/HICSS.2022.823.

Tekerek, M. (2008). Bilgi Güvenliği Yönetimi. *Kahramanmaraş Sütçü İmam Üniversitesi Fen ve Mühendislik Dergisi, 11*(1),132-137.

Soomro, Z. A., Shah, M. H., & Ahmed, J. (2016). Information security management needs more holistic approach: *A literature review. International Journal of Information Management, 36*(2), 215–225. https://doi.org/10.1016/j.ijinfomgt.2015.11.009

Vural, Y., ve Sağıroğlu, Ş. (2008). Kurumsal bilgi güvenliği ve standartları üzerine bir inceleme *Gazi Üniversitesi Mühendislik Mimarlık Fakültesi Dergisi*, *23*(2). 507-522.

Ahmed Baki ŞAFAK ve Demet SOYLU

Öğretim Görevlisi, Ankara Üniversitesi, Yönetim ve Organizasyon Bölümü, ahmedbakisafak@gmail.com
Dr. Öğr. Üyesi, Ankara Yıldırım Beyazıt Üniversitesi, Bilgi ve Belge Yönetimi Bölümü, bunchnoble@gmail.com