Türk Kütüphaneciliği, 36, 1 (2022), 74-89
Doi: 10.24146/tk.1012325

Belge Yönetimi ve Arşiv Uygulamalarının Bilgi Güvenliği İlkelerine Katkısı: Kavramsal Bir Değerlendirme

The Contribution of Records Management and Archival Practices to Information Security Principles: A Conceptual Review

Ceyhan Güler* **ve Fahri Furat****

Öz

Belge yönetimi ve arşiv uygulamaları tarih boyunca sürekli değişen, gelişen ve dönüşen alanlar olmuşlardır. Bu dinamizmin temel kaynağı olan teknolojik gelişmelerin son 30 yılda dijital teknolojiler ile birlikte kazandığı ivme bizi bir yanda daha kolay, daha yaygın, daha hızlı bir dünyaya taşırken bir yandan da yazılım ve donanım açısından risk ve tehditleri barındıran ve daha önce bildiğimizden çok farklı bir dünya ile karşı karşıya bıraktı. Kendisine uyum sağlayacak biçimde "değişmeye zorlayan" bu dünyada, teknolojilerden fayda sağlanması yerini gelişen teknolojiye uyum sağlamaya, eldeki birikimlerle bütünleşmeye ve sürece katkı vermeye bıraktı. ***Amaç****: Belge yönetimi ve arşiv uygulamalarının, bilgi güvenliği ilkeleriyle bütünleşmesi ve bu bağlamda daha güvenli belge yönetimi ve arşiv sistemlerinin ortaya çıkmasının sağlanması da bu sürece yapılacak bir katkı olacaktır.* ***Yöntem:*** Betimleme yönteminin kullanıldığı bu çalışmada belirtilen amaç çerçevesinde belge yönetimi ve arşiv uygulamalarının *"gizlilik, bütünlük ve kullanılabilirlik" üçlü bilgi güvenliği ilkeleriyle ilişkisi ele alınmış ve ISO 15489, TS 13298 gibi belge yönetimi ve arşiv uygulamalarını açıklayan standartlardaki ilkelerle, bilgi güvenliği standardı olan ISO 27001'deki ilkelerin ortak noktaları incelenmiştir.* ***Bulgular****: Yapılan değerlendirme, belge ve arşiv yönetimindeki ilke ve uygulamaların bilgi güvenliği ilkeleri ile benzer birçok yönünün olduğunu bize göstermektedir.* ***Sonuç:*** *Bu yönlerin bilgi güvenliğine katkıda bulunduğu, bu katkıyla beraber bilgi güvenliği standardının belge ve arşiv yönetimi ilke ve uygulamalarıyla bütünleşmesi gerekliliği ortaya çıkmaktadır. Değişen ve gelişen teknolojinin ve birlikte getirdiği potansiyel risk ve tehditlerin bütünsel bir stratejiyle ele alınması ancak her iki alanın katkılarıyla olası görünmektedir.* ***Özgünlük:*** *Bu çalışma belge ve arşiv yönetimindeki ilke ve uygulamalar ile bilgi güvenliği ilkelerini, her iki alanın ulusal ve uluslararası standartlarındaki yansımalarına bağlı olarak karşılaştırmaktadır. Belge yönetimi ve arşiv uygulamalarının, bilgi güvenliği ilkeleriyle bütünleşmesi ve bu bağlamda daha güvenli belge yönetim ve arşiv sistemlerinin ortaya çıkmasının sağlanması gerekliliğini ortaya koymakla özgün bir çalışma niteliğine sahiptir.*

Anahtar sözcükler: *Belge yönetimi; arşivcilik; bilgi güvenliği; risk ve tehditler; standartlar.*

* İstanbul Üniversitesi, Bilgi ve Belge Yönetimi Bölümü, İstanbul, Türkiye: E-posta: ceyhan.guler@istanbul.edu.tr
İstanbul University, Department of Information and Document Manageent, İstanbul, Turkey: E-mail: ceyhan.guler@istanbul.edu.tr
** İstanbul Üniversitesi, Bilgi ve Belge Yönetimi Bölümü, İstanbul, Türkiye: E-posta: mff@istanbul.edu.tr
İstanbul University, Department of Information and Document Manageent, İstanbul, Turkey: E-mail: mff@istanbul.edu.tr

Geliş Tarihi –*Received:* 20.10.2021
Kabul Tarihi – ***Accepted:*** 05.03.2022
Yayımlanma Tarihi – ***Published:*** 30.03.2022

Abstract

Records management and archival applications are fields that are constantly changing, developing and transforming throughout history. The acceleration of technological developments with digital technologies in the last 30 years has put us into an easier, more widespread and faster world. However, on the other hand, this new world carries enormous risks and threats in terms of software and hardware. In this world, which "forces change" to adapt to itself, the general understanding of benefiting from technologies has been replaced with adapting ourselves to the developing technologies, integrating with the knowledge at hand and contributing to this process. ***Objective:*** *The integration of records management and archival applications with information security principles and the emergence of more secure records management and archival systems in this context will also contribute to this process.* ***Method:*** *Based on the descriptive method, the connection between records management and archival applications with the triad information security principles of "confidentiality, integrity and availability" was discussed in this study. For this purpose, common points of the principles in the standards explaining records management and archival applications such as ISO 15489, TS 13298, and principles in ISO 27001, which are the information security standard, are discussed.* ***Findings:*** *The evaluation shows that the principles and practices in records and archival management have many aspects similar to information security principles.* ***Implications:*** *These aspects contribute to information security, and thus the necessity of integrating the information security standard with records and archival management principles and practices becomes a must. It seems possible with the contribution of both fields to address the risks and threats brought by changing technology and technology with a holistic strategy.* ***Originality:*** *This study compares the principles and practices in records and archival management with information security principles, depending on their reflections in the national and international standards of both fields, and ensuring the integration of records management and archival applications with information security principles, and in this context, the emergence of more secure records management and archival systems. It has the characteristic of an original work by revealing its necessity.*

Keywords: *Records management; archival science; information security; risks and threats; standards.*

Giriş

Bilgisayar sistemleri, günümüzde kamu kurum ve kuruluşlarının, özel işletmelerin ve bireylerin günlük işlerini ve faaliyetlerini yürüttüğü vazgeçilmez bir ortam haline gelmiştir. Söz konusu sistemlerin yaşamın her alanında bu şekilde yer alması, aslında sistemlere olan güvenimizin de göstergesidir. Sistemlere hem kurumsal hem de bireysel olarak sınırsız bilgi yüklenmesi, sistemlere olan güvenin ispatı olarak anlaşılabilir. Bu neredeyse sınırsız bilginin sistemlerde yer alması, sistemleri doğal olarak donanım ve yazılım kaynaklı risk ve tehditlere açık hale getirmektedir. Devletlerin, kurumların ve bireylerin sistemlerde karşılaşabilecekleri olumsuzluklara yönelik aldıkları tedbirler de aslında risk ve tehditlerle karşı karşıya olduklarının belirtisi olarak görülebilir.

1988'de Robert Morris'in ürettiği ilk internet "bilgisayar solucanı"nın bilgisayarları yavaşlatması (Morris Worm, 2022) ile başlayan ihlaller 1994 yılında, ABD Hava Kuvvetleri'nin

ana komuta ve araştırma tesisi olan Roma Laboratuvarı'na bir laboratuvar kullanıcısı gibi kimliği belirsiz kişiler tarafından yapılan yüzün üzerinde izinsiz giriş ve gizli dosyalara izinsiz erişim (U.S. Government Accountability Office, 1996) ile devam etti. 2007'nin başlarında bir Amerikan giyim ve ev eşyaları şirketi, yetkisiz bir bilgisayar sistemlerine izinsiz girişin kurbanı olduğunu ve bilgisayar korsanlarının kredi kartı, banka kartı, çek ve mal iade işlemleriyle ilgili verileri depolayan bir sisteme eriştiklerini duyurdu (Pepitone, 2014). 2010'da İran'ın Nükleer Santraline internetten gelen bir virüsün verdiği zarar tahmin edilenden çok daha tehlikeli sonuçlar doğurdu (Kelley, 2013). 2013'te bir bilgisayar korsanı Amerikan şirketlerinin bilgisayarlarına girerek önce 40 milyon kredi kartı ve ardından 2014'te 53 ila 56 milyon kredi kartı numarasını çaldı (Riley, Lawrence and Matlack, 2014). Nisan 2015'te, Birleşik Devletler Personel Yönetimi Ofisi, bir veri ihlaliyle karşılaştığını ve yaklaşık 21,5 milyon personel kaydının çalındığını farketti (Zengerle and Cassella, 2015). Temmuz 2015'te, bir hacker grubu, bir sosyal ilişler sitesinin kullanıcı verilerini aldıklarını iddia etti. Ardından, iddialarını kanıtlamak için şirketin CEO'sunun e-postalarını çöpe attı ve web sitesi kalıcı olarak kapatılmadığı takdirde müşteri verilerini dağıtmakla tehdit etti (Mansfield-Devine, 2015, s. 9). Haziran 2021'de, siber saldırı ABD'deki en büyük yakıt boru hattını ele geçirdi ve Doğu Kıyısı'nda yakıt krizi yarattı (Turton and Mehrotra, 2021).

Bilgisayar sistemlerinin ortaya çıkışı, onlara güvenin oluşması, gelişimleri ve yaygınlaşmaları kötü niyetlilere yeni bir mecra açarken diğer taraftan devletleri, hükümetleri onlara karşı meşru güvenlik tedbirleri geliştirmeye mecbur bırakmıştır. Geliştirilen tedbirler, zamanla suçlulara karşı güvenlik konusunda temel ilkelerin ortaya çıkmasını sağlamış ve bu ilkeler savunma mekanizmasının temellerine dönüşmüştür. Bir başka ifadeyle, tehdit ve risklere neden olan sebepler, bazı tedbir odaklı sonuçları doğurmuştur. Bu temel ilkeler, CIA triad (confidentiality, integrity, availability) olarak ifade edilen gizlilik, bütünlük ve kullanılabilirlik ilkeleri olarak şekillenmiştir. Gizlilik ilkesinin D. Elliott Bell ve Leonard J. La Padula'nın ABD Hava Kuvvetlerine güvenli bilgisayar sistemleri için sundukları çalışmaya[1] (Fruhlinger, 2020) bütünlük ilkesinin, David D. Clark ve David R. Wilson'ın (A Comparison of Commercial and Military Computer Security Policies) Ticari ve Askeri Bilgisayar Güvenliği Politikalarının Karşılaştırması (1987) adlı çalışmasına (Miller, 2010) ve son olarak kullanılabilirlik ilkesinin ise 1988 yılında yaşanan ve Morris Worm olarak adlandırılan bilgisayar solucanı vakasına dayanması muhtemel olarak görülmektedir (Miller, 2010). Bilgisayar sistemlerinin insan yaşamına girmesi, hemen beraberinde risk ve tehditleri de getirmiştir. Zamanla risk ve tehditlere karşı edinilen tecrübe, bilgisayar sistemlerindeki alınacak önlemler noktasında bütüncül bir yaklaşımın ele alınmasını gerekli kılmıştır.

CIA ilkelerinin belge yönetimi ve arşiv ilke ve uygulamalarıyla ilişkisi, her iki alanın sahip oldukları benzerlikler ortaya konularak değerlendirildiğinde belge yöneticilerinin ve arşivcilerin bilgi güvenliği konusunda bütüncül bir yaklaşım sergilemeleri gerektiği ortaya çıkacaktır. Söz konusu benzerlikler de, belge yönetiminde ve arşiv ilke ve uygulamalarında

[1] Orange Book olarak isimlendirilen ABD Savunma Bakanlığının *Trusted Computer System Evaluation Criteria* Kitabının takma adıdır. Orange Book, özellikle devlet satın alma sürecinde kullanılmak üzere farklı güvenlik sistemlerinin güvenliğini derecelendirmek için kriterler belirlemiştir. Orange Book'taki derecelendirmeler Bell - La Padula modeline göre yapılmıştır. Örneğin, C düzeyinde sınıflandırma, bilgisayar sisteminin isteğe bağlı erişim kontrolüne sahip olduğu anlamına geliyordu. Zorunlu erişim kontrolü için B seviyesi kullanılıyordu. Orange Book günümüzde yerini Common Criteria adı verilen uluslararası bir sisteme bırakmıştır (Orange Book, 2021).

başvurulan ISO 15489 ve TS 13298 ile bilgi güvenliği ilkelerinin bulunduğu ISO 27001 bilgi güvenliği standardının gizlilik, bütünlük ve kullanılabilirlik ilkeleri çerçevesinde karşılaştırmalı ve betimsel analiz yöntemleri ile tartışılmıştır.

Literatür Değerlendirmesi

Belge yönetimi ve bilgi güvenliği konusunu, bu çalışmada geliştirilen yaklaşımdan farklı olarak çeşitli çalışmalarda görmek mümkündür. Söz konusu çalışmaları, Türkiye'deki ve dünyadaki çalışmalar olarak iki kategoride yıllara göre sırasıyla inceleyebiliriz.

Türkiye'de, Çiçek (2011) tarafından yapılan çalışmada elektronik belgelerin özgünlüğünün korunamamasına değinmektedir. Özgünlüğün ise güvenirlik sorunu olduğunu çeşitli bilgi güvenliği programlarının bulunmasına rağmen tek başına güvenirlik sorununu çözemeyeceğini dolayısıyla bilgi güvenliği ile beraber arşivcilik bakış açısıyla da ele alınması gerektiğini ifade etmektedir (Çiçek, 2011, s. 88). Çalışmada bilgi güvenliği ve arşivcilik bakış açısının bütüncül olarak ele alınmasının, belgelerin ve belge sistemlerinin uzun süreli muhafazalarda gerekli olduğunun anlaşılması bilgi güvenliği ilkelerini destekleyici bir yaklaşım sergilemektedir.

Öztemiz ve Yılmaz (2013) tarafından bilgi kurumlarındaki bilgi güvenliği farkındalığına ilişkin yapılan çalışmada, belge yönetimi ve arşivcilik uygulamalarına değinilmemiş ancak kütüphaneler açısından dikkate değer sonuçlar ortaya konulmuştur. Bu çerçevede yetkisiz erişim, yasal olmayan veya sahte web sitelerinin ziyaret edilmesi gibi riskler sonucunda virüs saldırılarının kütüphanelerdeki başlıca tehdit olarak görülmesi, belge yönetimi ve arşiv uygulamaları için de önemlidir (Öztemiz ve Yılmaz, 2013, s. 94).

Yalçınkaya'nın (2015) yılında hazırladığı çalışmada güvenlik risklerinin, kurumların Elektronik Belge Yönetim Sistemlerindeki (EBYS) başarıyı etkileyen kritik bir unsur olarak görülmesi (Yalçınkaya, 2015, s. 31) önemlidir. Bu bakış açısı yabancı literatür kısmında da değindiği gibi iyi bir belge yönetim sisteminin bilgi güvenliği ilkelerine katkıda bulunacağı yargısını da desteklemektedir.

Yılmaz ve Özdemirci'nin (2019) yaptıkları çalışmada, EBYS'de bilgi güvenliğinin sağlanmasının önemi ve kurumlara rehberlik edilmesi amacıyla, bilgi güvenliği çerçevesinde EBYS'ler ele alınmış ve EBYS'ler için Bilgi Güvenliği Yönetim Sistemi (BGYS) Belgelendirme süreci tanımlanmıştır (Yılmaz ve Özdemirci, 2019, ss. 46-47).

Çakmak ve Eroğlu'nun (2020) hazırladıkları çalışmada, kurumların risk yönetimi uygulamaları çerçevesinde koruma uygulamaları değerlendirilmiştir. Söz konusu çalışmada, elektronik belge ve arşiv sistemlerinde risk değerlendirmesinin büyük bir kısmının bilgi güvenliği uygulamalarına dayandırılması ve süreç olarak görülmesi bu çalışmayı destekleyen noktalardır (Çakmak ve Eroğlu, 2020, s. 72).

Belge yönetimi ve bilgi güvenliği ile ilgili dünyadaki çalışmalara bakıldığında; Shaw ve Shaw (2006)'ın Electronic Records Management Criteria and Information Security adlı çalışması, Lomas'ın (2010) Information Governance: Information Security and Access within a UK Context isimli çalışması, Anderson'ın (2012) A Case for a Partnership Between Information Security and Records Information Management ve Henttonen'ın (2017) Privacy as

an Archival Problem and a Solution, Donaldson ve Bell'in (2019) Security, Archivists, and Digital Collections, başlıklı çalışmaları değinilmesi gereken çalışmalar arasındadır.

Shaw ve Shaw (2006), bir kişi, şirket veya hükümetin tahkim altında eylemlerini haklı gösterebilmesi için makul bir gerekliliği olduğunu ve bu gerekliliğin uygunluğunu göstermek, anlaşmazlıkları çözmek ve gerektiğinde maliyet ve sorumluluğu tahsis etmek için kullanılabilecek belge yönetimi ve arşiv uygulamalarının önemine vurgu yapmaktadır. Bilgi altyapısının güvenlik özelliklerini ise, kullanılabilirlik, bütünlük ve gizlilik ilkeleriyle açıklayan Shaw ve Shaw (2006, ss. 137-144), bu özelliklerin belge yönetimi ve arşiv uygulamaları tarafından ele alınan gereklilikler olduğunu söylemektedir. Dolayısıyla belge yönetimi ve arşiv uygulamalarının bilgi güvenliği ilkeleriyle birlikte ele alınması temel yaklaşım olarak görülmüştür.

Lomas'ın (2010) çalışması bilgi güvenliği ilkeleri olan gizlilik, bütünlük ve kullanılabilirlik ile ISO 15489 arasındaki benzerlikleri ele alması ve belge yönetimi ve arşiv uygulamalarının uluslararası standartlara nasıl yansıdığını özellikle ISO 15489 ve ISO 27001 karşılaştırmalı göstermesi açısından önemlidir (Lomas, 2010, s. 190).

Anderson (2012) çalışmasında bilgi güvenliği ve belge yönetimi arasında sağlam bir ilişki geliştirmeye yönelik bir yaklaşıma vurgu yapması ve bilgi güvenliği uzmanları ile belge yöneticilerinin beraber çalışması gerektiğini ifade etmesi (Anderson, 2012, ss. 40-44) çok önemlidir.

Henttonen (2017), belge yönetimi ve arşiv uygulamalarının, tam olarak bilgiyi bir bağlamdan ve zamandan başka bir bağlam ve zamana kullanılabilir ve anlaşılır biçimde aktarmak için var olmaları nedeniyle gizlilik konularının odak noktasında olduğunu değerlendirmiştir (Henttonen, 2017, s. 4).

Donaldson ve Bell (2019), bilgi güvenliği ilkelerinin arşivcilik için önemini vurgularken, hem bilgisayar uzmanlarının hem de arşivcilerin güvenlik gereksinimleri, sistemlerini her türlü zarardan korunmasını sağlamayı vurgulamaları bakımından benzer olduğunu ifade etmektedirler. Arşivcilik açısından dijital hırsızlığın aşina olunan bir durum olmadığını ancak bunun da öğrenmeye başlandığı açıklanmıştır. Arşivciliğin aşina olmadığı veya aşina olunmaya çalışıldığı dijital hırsızlık konusunda bilgisayar biliminin, dijital hırsızlık konusunda çalışma geleneğine sahip olduğunun ortaya konması bilgi güvenliği ilkelerinin ele alınmasındaki önemi ortaya koymaktadır (Donaldson ve Bell, 2019, ss. 5-6).

Bunlar dışında NSW Government State Archives and Records (Yeni Güney Galler)'un (2019) çevrimiçi olarak yayımlanan How Records and Information Management Techniques and Skills Can Contribute to Information Security Objectives adlı çalışmada ise iyi bir belge yönetimi sisteminin bilgi güvenliğine katkıda bulunabileceğinin ifade edilmesi önemlidir (NSW Government State Archives and Records, 2019).

Araştırmanın Kapsamı, Amacı ve Yöntemi

Araştırmanın kapsamı, belge yönetimi ve arşiv uygulamalarının standart çerçevesini belirleyen ISO 15489, TS 13298 ve bilgi güvenliği standardı ISO 27001'de tanımlanan "gizlilik, bütünlük ve kullanılabilirlik" ilkeleridir.

Bu çalışma belge ve arşiv yönetimindeki ilke ve uygulamalar ile bilgi güvenliği ilkelerini, her iki alanın ulusal ve uluslararası standartlarındaki yansımalarına bağlı olarak karşılaştırmaktadır. Ayrıca, belge yönetimi ve arşiv uygulamalarının, bilgi güvenliği ilkeleriyle bütünleşmesi ve bu bağlamda daha güvenli belge yönetim ve arşiv sistemlerinin ortaya çıkmasının sağlanması gerekliliğini ortaya koymakla özgün bir amaca sahiptir. Tüm yaşam ve çalışma alanlarını "değişime zorlayan" bu dünyada bu bütünleşmenin gerçekleşmesi ve daha güvenli sistemlerin ortaya çıkması çalışmamızın orijinallik değerini arttıracak ve alanyazına önemli bir katkı sağlayacaktır.

Bu çalışmada, belge yönetimi ve arşiv uygulamalarının çerçevesini belirleyen ISO 15489 ve TS 13298 standartlarındaki ilkelerle bilgi güvenliği standardı olan ISO 27001'deki "gizlilik, bütünlük ve kullanılabilirlik" üçlü bilgi güvenliği ilkesinin ilişkisini ele almak ve ortak noktalarının karşılaştırmasını sağlamak için betimleme yöntemi kullanılmıştır. Söz konusu yöntem, geçmişteki veya günümüzdeki bir vaziyete hiçbir şekilde karışmadan neden sonuç ilişkisini olduğu gibi tanımlamayı amaçlayan araştırma modelidir (Karasar, 2012, s. 77). Betimleme, değişkenleri ve değişkenler arasındaki ilişkileri belirlemeyi, düzenlemeyi ve kayıt altına almayı amaç edinir (Neuman, 2008, s. 22). Betimleme yöntemi belge yönetimi ve arşiv uygulamaları için faydalı hale gelen değişikliklerin ölçeğine ve kapsamına atıfta bulunmaya izin veren bir dizi seçilmiş temel kriterleri ve ayrıca değişimin ileri yönleriyle ilgili tavsiyeleri değerlendirmektedir. Böylelikle belge yönetimi ve arşiv uygulamaları ile bilgi güvenliği ilkelerinin işlevselliğini açıklayan faktörler ele alınmıştır.

Belge Yönetimi ve ISO 15489, TS 13298

Dünyada farklı ülkelerde kamu kurum ve kuruluşlarında belge yönetim süreçleri, tercih edilen ortama bağlı olarak kâğıt, elektronik veya hibrit bir biçimde yürütülebilmektedir (Association for Information and Image Management International [AIIM], 2009, s. 11). Hong Kong'ta belgelerin hibrid ortamda yönetimi için rehberler de hazırlanmıştır (The Government of Hong Kong Special, 2020). Ülkemizde ise 2020 yılında yayımlanan Resmi Yazışmalarda Uygulanacak Usul ve Esaslar Hakkında Yönetmelikle belgelerin elektronik ortamda üretilmesi asli unsur haline gelmiştir (Resmi Yazışmalarda Uygulanacak, 2020). Geleneksel anlamda, belgelerin üretilmesi, düzenlenmesi/tanımlanması, kullanımı, değerlendirilmesi, imha edilmesi veya süresiz olarak korunmak üzere arşive devri, kurumlarca yıllardan beri yapılan uygulamalardır. Internet kullanımının yaygınlaşması, standartlarla belirlenmiş elektronik belge yönetim sistemlerinin benimsenmesi ve kullanımı, geleneksel anlamdaki belge yönetimi ve arşiv uygulamalarının da elektronik ortama taşınmasının önünü açmış ve elektronik ortamdaki bilgi üretimini önemli kılmıştır. Özellikle 2000'li yıllardan sonra yapılan yasal değişiklikler, elektronik ortamdaki üretimin meşru bir çerçeveye oturmasını sağlamıştır. Belge yönetimindeki uluslararası gelişmeler ve uygulamalar, elektronik belge yönetiminin hem mevzuat hem de kurumsal tabanlı yaklaşımların sınırlarını belirleyen standartların kullanımı, Türkiye'deki kurumların elektronik belge yönetim sistemlerine olan güvenini uzun süren bir kamu direnci ve buna bağlı olarak siyasi idarenin konuyu sahiplenmesi ile zamanla artırmıştır. Dolayısıyla dünyada yaygın olarak kullanılan Avustralya tabanlı olan ve daha sonra ISO tarafından kullanılan 15489, Türkiye'de de kabul görmüştür ve Türk Standardı olarak hem özel kurumlardaki hem de kamu kurumlarındaki kullanıcılar tarafından üretilen belgelerin

yönetilmesine yardımcı olması amacıyla Türkçe'ye çevrilmiştir (Türk Standardları Enstitüsü [TSE], 2021). Başta ISO 15489 olmak üzere, Avrupa Birliği belge yönetim modeli olan MoReq ve devamı olan MoReq2, İngiltere ulusal arşivinin hazırladığı belge yönetim gereklilikleri gibi uluslararası çerçeveye sahip olan düzenlemeler, TS 13298 standardının hazırlanmasında etkili olmuştur. TSE tarafından 19 Haziran 2007 tarihinde "TSE 13298 Bilgi ve Dokümantasyon-Elektronik Belge Yönetimi" adı ile standart olarak kabul edilmişti (Kandur, 2006; Önaçan, Medeni ve Özkanlı, 2012, s. 8; TS 13298, 2009; aktaran Eroğlu ve Külcü, 2014, s. 335). 2008/16 sayılı Başbakanlık Genelgesi ile kamu kurum ve kuruluşlarının oluşturacakları elektronik belge yönetim sistemlerinde TSE 13298 no'lu standarda göre işlem yapmaları ve söz konusu Genelgenin yayımlanması öncesi kurulan sistemlerin de ilgili kamu kurum ve kuruluşlarınca gözden geçirilerek iki yıl içinde Standarda uyumlu hale getirilmesi istenmiştir (Başbakanlık Genelgesi, 2008). 2015 yılında güncellenen TS 13298, günümüzde TSE tarafından sertifikalandırılmak üzere yazılım firmalarının kamu kurumlarındaki belge yönetim yazılımı ihtiyacının karşılanması için söz konusu standart için lisans vermektedir.

ISO 15489'un dünya genelinde kabul görmüş ve ilk uluslararası belge yönetim standardı olması (Stephens, 2001, s. 68; aktaran Külcü, 2007, s. 238), TS 13298'in de ulusal bir nitelik taşıması bilgi güvenliği ilkelerinin hem ulusal hem de uluslararası olarak belge yönetimiyle ilişkisinin ortaya konması açısından önemlidir.

Belgelerin elektronik belge yönetimi sistemleriyle üretilmesi ve korunması, ilgili standartlarda tanımlanmıştır. Bu tanımlamalarda, belgelerin güvenliğinin yeterince sağlanıp sağlanamadığı bilgi güvenliği standardıyla olan ilişkinin bilinmesiyle belirlenebilir. Söz konusu ilişki, her iki disiplinin temel standartlarının karşılaştırılmasıyla mümkün olabilir.

Bilgi güvenliğine yönelik tanımlamalara baktığımızda, TS ISO 15489 nolu enformasyon ve dokümantasyon – belge yönetimi standardında orijinallik, güvenirlilik, bütünlük ve kullanılabilirlik ilkeleri tanımlanmıştır (International Organization for Standardization [ISO], 2001 s. 12; TSE, 2019, s. 12). Söz konusu ilke tanımları TS 13298'de; sırasıyla erişim hakları, bütünlük açıklamaları ve kullanım açıklamaları olarak yer almaktadır. Bahsedilen tanımların ayrıntılı açıklamaları çalışmanın "belge yönetimi ve bilgi güvenliği arasındaki ilişkinin değerlendirilmesi" başlığı altında verilmiştir.

Türkiye'de TS 13298'deki ilkeler dışında, EBYS ile uyumlu ve tercih edilebilecek orta seviyeli güvenlik sorunlarına yönelik hazırlanan koruma profili, belge yönetimi ve arşiv kurumları için bilgi güvenliğini sağlamada yardımcı önemli web tabanlı elektronik doküman ve belge yönetim sisteminin varlığı da söz konusudur (TSE, 2014). Profilde tanımlanan tehditler; yetkisiz erişim, veri değişimi, inkâr edilebilirlik, bilginin izinsiz ifşa edilmesi, sistemin erişilemez ve kullanılamaz olmasını sağlama, zararlı veri ve çeşitli tehditler kullanılarak elde edilen kısıtlı erişimdir. Koruma profili, bilginin bütünlüğü, denetimi ve belge ile ilgili tüm bilgiler üzerindeki herhangi bir yöntemle bilgi değişikliğini belirlemeyi ve olası değişikliklere karşı tedbirler almayı garanti etmektedir (TSE, 2014, s. 26).

TS 13298 dokümanında, her ne kadar elektronik belgelerin üretim ortamına ait bilgi güvenliği ile ilgili herhangi bir kriterin kapsanmadığı ifade edilmiş (TSE, 2015, s. 9) olsa da, TS ISO/IEC 27001'deki temel unsurlara yardımcı ilkelere sahiptir. Bu ilkeler, söz konusu bilgi güvenliği standardında, bilginin gizliliği, bütünlüğü ve kullanılabilirliği ilkeleriyle bilgi

güvenliğine ilişkin risklerin yönetildiği ilkelere yardımcı olmaktadır (ISO, 2005, s. V). Üçlü ilkenin, belge sistemlerine yönelik güvenlik riskleri:

- Belgelere müdahale edilmesi,
- Belgelerin uygun olmayan şekilde değiştirilmesi,
- Belgelerin uygun olmayan şekilde imha edilmesi,
- Belgelerin uygun olmayan yerde bulunması ve
- Belgelere yetkisiz kişilerce erişimin olmasıdır.

Belgelerin sıralanan risklere karşı korunmasına yönelik bilgi güvenliği standardında kayıtların, kayıp, imha, tahrifat, yetkisiz erişim ve yetkisiz salıverilmeye karşı korunacağı ifade edilmektedir (ISO, 2005, s. 21).

Kurumdan kuruma farklılık gösterse de söz konusu problemlerin yaşandığı bazı alanlarda daha fazla hassasiyet gerekmektedir. Bir sağlık kuruluşundaki bir belgenin istenmeyen değişikliğe uğraması hem kişi sağlığı açısından hem de kurumsal imaj noktasında büyük kayıplara yol açabilir. Bir bankanın müşteri bilgilerinin çalınması gizlilik açısından büyük problemlere dolayısıyla mali kayıplara yol açabilir. Hastane ve banka örneği buralardaki belge üretiminde bilgi güvenliği ilkelerinin ne kadar önemli olduğunu göstermesi açısından dikkate değerdir. Bilgi güvenliği, bilginin sadece bu kurumlarda değil, tüm kamu kurum ve kuruluşlarında ve özel tüzel kişilik kurumlarında her türlü saldırıya karşı korunmasını gerekli kılmaktadır. Kurum ayrımı olmaksızın belge yöneticilerinin ve arşivcilerin bulundukları kurumdaki elektronik belge yönetim sistemlerine bağlı güvenlik risklerini bilme yeterliliği, bilgi güvenliğinin nasıl sağlaması gerektiğini bilmesi noktasında çok önemlidir.

Bilgi Güvenliği ISO 27001

Bilgi, teknolojinin gelişimi ve yaygın kullanımıyla beraber hem kişilerin hem de kurumların vazgeçilmez önemli bir varlığı haline geldi. Bilgi güvenliği, bilgi ve bilgi sistemlerinin gizlilik, bütünlük ve kullanılabilirliğini sağlamak için yetkisiz erişim, kullanım, açığa çıkarılma, bozulma, değişiklik veya imhadan korunması olarak tanımlanabilir (Nieles ve diğerleri, 2017, s. 2). Bilgi güvenliği, bilginin her türlü risk ve saldırıya karşı korunması için birçok önlem alınmasını içermektedir (Canbek ve Sağıroğlu, 2006). Örneğin bilgilerin elektronik ortamlarda transferi ve depolanması aşamalarında meşru olmayan kullanımlardan ve yetkisiz erişimlerden korunması bilgi güvenliği çerçevesinde değerlendirilir. Bunun yanında bilgi güvenliği, güvenilir bir bilgi ve belge sisteminin meydana getirilmesi ve söz konusu sistemin veya bilgi ve belgenin yetkisiz ve ilgisiz kişi ya da kişilerce erişilmesini önleyici tedbirleri ve çabaları da ifade eder (Seferoğlu ve diğerleri, 2018, s. 31). Dolayısıyla, bilgi güvenliği birçok tehdidin önlenmesine yardımcı olmaktadır. Ancak bilgi güvenliği risk ve tehditleri teknolojinin gelişim hızıyla paralel olarak çeşitlenmektedir (Seferoğlu ve diğerleri, 2018, s. 32). Bu nedenle, bilgi güvenliği standardı olan ISO 27001'in iyi anlaşılması gerekmektedir. Nitekim bilgi güvenliğiyle ilgili tehditler, bilgi ve belgenin gizliliğini, bütünlüğünü ve kullanılabilirliğini bozacak risk ve tehditler olarak değerlendirilebilir (Blanding, 2004; aktaran Seferoğlu ve diğerleri, 2018, s. 34). Belirtilen gizlilik, bütünlük ve kullanılabilirlik ilkeleri, ISO 27001'de benimsenmiştir.

Bilgi güvenliğinin ilk ilkesi olan gizlilik, hassas bilgilere yetkisiz erişimi engellemekle ilgilidir. Erişim, bir saldırganın ağa girmesi ve bilgileri okuması gibi kasıtlı olabilir veya

bilgileri kullanan kişilerin dikkatsizliği veya yetersizliği nedeniyle kasıtsız olabilir (Brooks, 2019). Gizlilik, kişisel gizliliği ve özel bilgileri koruma araçları da dâhil olmak üzere, bilgi erişimi ve ifşası üzerindeki yetkili kısıtlamaları korumaktır. Gizlilik kaybı, bilgilerin yetkisiz olarak ifşa edilmesidir. Gizlilik ilkesi, iki temel kavram üzerine şekillenmektedir. Bunlar; veri güvenliği ve mahremiyettir. Veri güvenliği, özel veya gizli bilgilerin yetkisiz kişilere verilmemesini veya ifşa edilmemesini sağlar. Mahremiyet ise bireylerin kendileriyle ilgili hangi bilgilerin toplanıp saklanabileceğini ve bu bilgilerin kimler tarafından ve kime ifşa edilebileceğini kontrol etmelerini veya etkilemelerini sağlar (Stallings ve Brown, 2015, s. 13).

Bilgi güvenliğinde bütünlük ilkesi, yetkisiz kullanıcılar tarafından bilgilerin değiştirilmesinin engellenmesi, yetkili kullanıcılar tarafından yetkisiz veya kasıtsız bilgilerin değiştirilmesinin önlenmesi ve iç ve dış tutarlılığının korunması amaçlarını taşır (Brooks, 2019). Bütünlük, bilgilerin reddedilmemesini ve güvenilirliğini sağlamak da dâhil olmak üzere uygunsuz bilgi değişikliği veya imhasına karşı koruma sağlamaktır. Bütünlük kaybı, bilgilerin yetkisiz olarak değiştirilmesi veya imha edilmesidir. Bütünlük ilkesi de iki temel kavramda ele alınır. Bunlar; veri bütünlüğü ve sistem bütünlüğüdür. Veri bütünlüğü, bilgi ve programların yalnızca belirtilen ve yetkilendirilmiş bir şekilde değiştirildiğini garanti eder. Sistem bütünlüğü ise bir sistemin amaçlanan işlevini, kasıtlı veya kasıtsız yetkisiz manipülasyondan uzak bir şekilde, yerine getirmesini sağlar (Stallings ve Brown, 2015, s. 13).

Bilgi güvenliğinin son ilkesi olan kullanılabilirlik ise bir sistemin yetkili kullanıcılarının sistemdeki bilgilere ve ağa zamanında ve kesintisiz erişime sahip olmasını sağlar (Brooks, 2019). Sistem çökmesi, virüs vb. nedenlerle ihtiyaç duyulan bilgiye erişim sağlanamaması durumunda, başvurulması gereken yöntemlerin bilinmesi söz konusu ilke kapsamındadır.

Belge Yönetimi ve Bilgi Güvenliği Arasındaki İlişkinin Değerlendirilmesi

ISO 27001 sistemini uygulamak, sistem kapsamındaki bilgi varlıklarını üç temel bilgi güvenliği gereksinimine karşı risk değerlendirmesi yapmaktır. Risk değerlendirmesi, bir bilgi varlığının gizliliğini, bütünlüğünü ve bilginin kullanılabilirliğini tehlikeye atacak risklerin değerlendirilmesini gerektirir. Bu tanımlar, kullanılabilirlik, bütünlük, güvenilirlik ve özgünlük kaydı için ISO 15489 karakteristik gereksinimleriyle önemli bir görev benzerlik ilişkisine sahiptir (Lomas, 2010, ss. 190-191). Söz konusu ilişki, ISO 15489'a da dayanan TS 13298 için de geçerlidir. Standartlar arasındaki ilişki aşağıdaki tabloda verilmektedir.[2]

[2] Söz konusu ilkeler, ilgili oldukları standardın temel çerçevesini oluşturduğu için, standartların belirli yıllardaki revizyonlarında da aynı şekilde aktarılmaktadır. Bu nedenle ISO 27001'in 2005 yılından sonra yapılan 2013 ve 2017 revizyonlarında; ISO 15489'un 2001 yılından sonra yapılan 2016 revizyonunda; TS 13298'in 2009 yılından sonraki 2015 revizyonunda çalışmanın kapsamındaki ilkelerde değişiklik görülmemiştir.

Tablo 1

ISO 27001 ile ISO 15489 ve TS 13298 arasındaki görev benzer ilişkisi

ISO 27001	ISO 15489	TS 13298
Gizlilik Bilginin yetkisiz kişilere, kuruluşlara veya süreçlere sunulmadığı veya ifşa edilmediği özellik.	**Gizlilik** ISO 15489-1'in bütünlükle ilgili 8.2.3 Bölümü, 'yetkisiz erişimi, kayıtların yok edilmesini, değiştirilmesini veya kaldırılmasını önlemek için erişim izleme, kullanıcı doğrulama, yetkili imha ve güvenlik gibi kontrol önlemlerinin mevcut olduğunu' gerektirir (ISO, 2001, s. 9). ISO 15489'un ek bölümleri, denetim, koruyucu etiketleme, izleme ve güvenli depolama dâhil olmak üzere kontrolün diğer yönleri için hükümler sağlar,	**Erişim Hakları** EBYS, bünyesinde yer alan elemanlar için en azından beş kademeli erişim hakları tanımlayabilmelidir. Bunlar: **Tasnif dışı:** içerdiği konular itibariyle, gizlilik dereceli bilgi taşımayan, bilgi, belge, evrak, mesaj ve dokümanlara verilen haklardır. **Hizmete özel:** içerdiği konular itibariyle, gizlilik dereceli konular dışında olan, güvenlik işlemine ihtiyaç gösteren ve Devlet hizmetine ait özel bilgileri ihtiva eden bilgi, belge, evrak, mesaj ve dokümanlara verilen gizlilik derecesidir, **Özel:** İçerdiği konular itibariyle, izinsiz olarak açıklandığı takdirde, milli menfaatlerimizi olumsuz yönde etkileyecek olan bilgi, belge, evrak, mesaj ve dokümanlara verilen gizlilik derecesidir. **Gizli**: Müsaadesiz olarak açıklandığı takdirde, ulusal güvenliği, milli prestij ve menfaatlerimizi ciddi ve önemli derecede zedeleyecek olan bilgi, belge, evrak, mesaj ve dokümanlara verilen gizlilik derecesidir. **Çok gizli:** Müsaadesiz olarak açıklandığı takdirde, ulusal güvenliği büyük ölçüde tehlikeye düşürecek, Devletimize ve müttefiklerimize büyük ölçüde zararlar verebilecek olan bilgi, belge, evrak, mesaj ve dokümanlara verilen gizlilik derecesidir.

Bütünlük Varlıkların doğruluğunu ve tam olmasını koruma özelliği.	**Bütünlük** Bir belgenin karakteristik özellikleri; tamamlanmış olması ve değiştirilmemiş olmasını gerektirir.	**Bütünlük** Elektronik belgelerin bütünlüğünü korumalı ve söz konusu belgelerin bütünlüğünün sorgulandığı durumlarda bütünlüğün bozulmadığını gösterebilmelidir. Bütünlük kavramı elektronik belgenin entelektüel (içerik), tanımsal ve fiziksel olarak bir bütün olarak korunmasıdır.
Kullanılabilirlik Bilgi varlıkları, yetkili bir kuruluş tarafından talep edildiğinde erişilebilir ve kullanılabilir olmalıdır.	**Kullanılabilirlik** Bir belge; yerinin belirlenmiş olmasını, erişilebilmesini, anlaşılmasını ve yararlanılmasını gerektirir.	**Kullanım** TS 13298'in 8. Bölümünde EBYS'lerin kullanım özelliklerini belirten bir elemanın aranması, görüntülenmesi ve yazdırılması durumları EBYS fonksiyonelliği açısından gereklidir. Bu özellik bir belgenin yerinin olmasını ve erişilebilir olmasını gerektirmektedir.
Orijinallik Standart bağlamında 'bilgi güvenliğinin' kapsayıcı tanımı şudur: "bilginin gizliliğinin, bütünlüğünün ve kullanılabilirliğinin korunması; ek olarak, özgünlük, hesap verebilirlik, inkâr edilemezlik ve güvenilirlik gibi diğer özellikler de söz konusu olabilir" (ISO, 2005, s. 2). Bu, bilginin 'gerçek' olduğuna dair kanıt sağlanmasını çevreleyen ek gereksinimleri tanır ve böylece gereksinimin sistem geliştirmesine dâhil edilmesini sağlar.	**Orijinallik** Bir belgenin; iddia ettiği gibi olduğu kanıtlanmış, iletilmesi için yazarlık ve/veya sorumluluk iddiasında bulunan kişi tarafından oluşturulduğu veya gönderildiği kanıtlanmış, belirtilen zamanda oluşturulduğu/veya gönderildiği kanıtlanmış olmasını gerektirir.	**Orijinallik** Belgelerin üretildiği dönemdeki içerik, ilişki ve sunum özelliklerinin korunması için gerekli tedbirlerin alınması gereklidir.

Açıklama notu: Tablodaki ISO 27001 ve ISO 15489'un karşılaştırması, "Lomas, E. (2010). Information governance: Information security and access within a UK context. *Records Management Journa*l, *20*(2), 190" kaynağına dayanmaktadır.

Bilgi güvenliği açısından olaya bakıldığında kullanılabilirlik ilkesinin var olabilmesi için provenans ve üstverinin güvenli olması şarttır. Provenans ve üstverinin güvenliği ise bilgi güvenliği ilkelerinin sağlanmasından geçmektedir. Kullanılabilirlik ilkesinde, belge yönetimi ilkeleri ve bilgi güvenliği ilkeleri bütüncül bir şekilde birbirini desteklemektedir. Birinin varlığına tehdit diğerinin de aynı tehdide maruz bırakılmasının yolunu açmaktadır. Belgelerin herhangi bir şekilde davaya söz konusu olması veya adli bilişim için kanıt olarak kullanılabilirliği de belge yönetiminin bilgi güvenliğine hizmet ettiğini göstermektedir. Özellikle üstverilerin kullanım kontrolünü gerçekleştirmek üzere belgenin yaşam döngüsü boyunca kullanılması gerçekleştirilen eylemlerin izlenebilirliğinde kolaylık sağlamaktadır (Munier ve diğerleri, 2020, s. 6).

Tartışma, Sonuç ve Öneriler

Kurumsal ve bireysel bilginin güvenliği, teknolojik yeniliklerin sunduğu araçlarla beraber karşılaştığı risk ve tehditler zaman geçtikçe daha büyük bir problem haline gelmektedir. Bilgi üretiminin sanal ortama taşınmış olması kurumlara ve bireylere ait bilgilerin saldırganlar tarafından hedef alınmasını kolaylaştırmaktadır. Hem kurumsal hem de kişisel verilerin saldırganların hedefinde olmasının birçok nedeni olabilir. Devletler arası gizli savaşların bilgi teknolojileri üzerinden sürdürülmesi, küresel çaptaki firmaların rekabet mücadelesi ve bilgi, belge bazlı şirketlerin ticari amaçları vb. durumlar söz konusu nedenlerin başında gelmektedir (Seferoğlu ve diğerleri, 2018, s. 33). Öte yandan bilgi güvenliği odaklı bilimsel çalışmaların sunulması, hem bireylerin hem de kurumların bilgi güvenliği dinamiklerini destekleyecek ve hizmet içi veya bireysel eğitimlerin bilgi güvenliğini destekleyecek şekilde tasarlanmasına yardımcı olması açısından yararlıdır (Seferoğlu ve diğerleri, 2018, s. 35).

Bilgi güvenliği, risklerin neden olduğu birer sonuç olarak karşımıza çıkmaktadır. Bu nedenle gizlilik, bütünlük ve kullanılabilirlik sebeplerin senteziyle ortaya konulan önemli bilgi güvenliği ilkeleridir.

Belge yönetimi ve arşiv uygulamaları kapsamında gizlilik ilkesini değerlendirdiğimizde, belge yönetimi teknik ve yasal düzenlemelerinde, belgelerin üretilmesi aşamasında, belgenin erişim haklarının tanımlanmış olması zorunludur. Bu haklar; tasnif dışı, hizmete özel, özel, gizli ve çok gizli olmak üzere beşe ayrılmaktadır. Bu haklar belgenin gizliliği noktasında belge üreten kişiye yardımcı olmaktadır. Ayrıca, belge yöneticisinin ve arşivcinin de bu durumdaki belgelere bu haklar çerçevesinde bakılmasını da sağlamaktadır.

Bununla beraber "Özel" ve üstü gizlilik dereceli belgelerin üretimi, düzenlenmesi, tanımlanması, transferi, depolanması ve diğer belge yönetimi ve arşivcilik uygulama işlemleri ilgili yasal düzenlemeye bağlı olarak fiziksel ortamda gerçekleştirilmesi yönetmelikte belirtilmiştir (Resmi Yazışmalarda Uygulanacak, 2020). Dolayısıyla belge yönetimindeki erişim hakları bilgi güvenliğindeki gizlilik ilkesini sağlamaya yardımcı olmaktadır. Bu noktada belge yöneticileri ve arşivcilerin farkında olması gereken husus belgenin erişim hakkının belgenin imza yetkisindeki kişilerin bunu belirlemek zorunda olduklarıdır (Resmi Yazışmalarda Uygulanacak, 2020). Bilgi güvensizliği anlamında gizlilik ilkesi, yetkili kişilerin şifrelerini basit ve karışık olmayacak şekilde belirlemeleridir. Ayrıca, mobil üzerinden bu şifrelerin kullanılması hücresel verinin güvenliği yanında wi-fi kullanımı daha da büyük bir problem olarak karşımıza çıkabilir. Bu nedenle gizlilik ilkesindeki bilgi güvensizliği kişilerin yeterli tedbirleri alamamasıdır. Bunun yanında bulut bilişimdeki bilgilerin nasıl düzenleneceği bulut servis sağlayıcılarıyla gerekli prosedürlerin nasıl uygulanması gerekliliğinin bilinmemesi, bilgi güvensizliğine yol açabilecek bir konudur.

Belge yönetimi ve arşiv uygulamaları kapsamında bütünlük ilkesi, TS 13298'de elektronik belgelerin içeriksel, tanımlayıcı özellikleri ve fiziksel nitelikleri olmak üzere tamamlayıcı bir şekilde korunmasını ifade etmektedir. İçeriksel bütünlük, belgenin içeriğine hiçbir şekilde müdahale edilmesine imkân verilmemesidir. Ayrıca, belgelerin erişilebilir, okunabilir ve yorumlanabilir olmasını da sağlamaktadır. Bunlar, provenans prensibi ve asli düzen prensibi ile yerine getirilmektedir. Provenans, üretilen bir belgenin kaynağına gitmesine yardımcı olmaktadır. Kaynak, kurum veya kişi olabilmektedir. Ayrıca, bu prensibe göre düzenlenip tanımlanan bir belgenin değişikliğe uğraması da zordur. Çünkü her kamu dairesi bir

idari birimdir ve her birime ait belgeler, idari birimin faaliyetlerini yansıtan homojen bir grup oluşturur. Bu büyük grup, doğal olarak alt gruplara ayrılır ve alt gruplar, birimin bağlı olduğu kurumu ve işlevlerini izleyerek seriye ayrılır. Bu durumda belgeleri üreten kurum ve faaliyetlerin açıkça yansıtıldığı bir sınıflandırma gerekliliği vardır. Bu sınıflandırmadaki düzensizlik, belgenin üretildiği idari yapıya uymayacağı için bütünlük ilkesine de yansımaktadır (Schellenberg, 1951). Zamanla asli düzen prensibini de içine alan provenans ilkesi dış ve iç olmak üzere iki ayrı yapıya sahip olmuştur. Dış yapıda hiçbir şekilde müdahale söz konusu olmazken iç yapıda belge yöneticisinin ve arşivcinin müdahale hakkı söz konusudur (Yıldız, 2006, s. 7). Özetle provenans ilkesi sahip olduğu dış ve iç yapı ile belgelerin bütünlüğünü sağlamaya yardımcı olmaktadır. Böylelikle bütünlük ilkesi kapsamında bilgi güvenliğini sağlayıcı yardımcı bir rol üstlenmektedir. Bütünlük ilkesinde, belge yöneticilerinin ve arşivcilerin kurum ve kişileri işlevlerinin sonucu olan belgelerle uygun bir şekilde yansıtmaları gerekliliği, provenansın güvenliği açısından önemlidir. Ayrıca, belge üretim aşamasında, belgenin üretimine katkıda bulunan bilginin (taslak metin, mail, mesaj vb.) korunması noktasında, belge yöneticilerinin ve arşivcilerin belge üretiminin nihai sahibi olan kurumsal bağlamdaki kişilere konuyla ilgili farkındalık oluşturacak araçlar geliştirmek gibi görevlerinin olması muhtemeldir.

Belge yönetimi ve arşiv uygulamaları kapsamında kullanılabilirlik ilkesi, EBYS kapsamındaki varlıkların aranması, görüntülenmesi ve yazdırılması gibi erişim ve kullanım özellikleri olarak düşünülebilir. Ayrıca, kullanılabilirlik ilkesiyle ilişkili olabilecek problemler için felaket kurtarma planları yer almaktadır. Planlar, genellikle sistemin belirli periyotlarla yedeklenmesinin sağlanmasını gerekli kılmaktadır. Sadece felaket kurtarma programları değil, bilginin nerede depolandığı, süresiz olarak saklanan belgelerin nasıl korunacağı ve bunlara erişim gibi problemler de kullanılabilirlik ilkesi kapsamında düşünülmesi gerekmektedir.

Belge yönetimi ve arşivcilikte erişime ilişkin sınıflandırmalar, bilgi güvenliğinin gizlilik ilkesinin sağlanmasında yardımcı olduğu gibi aynı şekilde provenans ve üstveriler de bilgi güvenliğinin bütünlük ve kullanılabilirlik ilkelerini sağlamada yardımcı olduğu muhtemeldir. Ancak söz konusu belge yönetimi ve arşivcilik prensipleri her ne kadar bilgi güvenliğini sağlamada yardımcı olduğu söylense de, yardımcı olma vasfının, belgenin güvenliğiyle ilgili olduğu görülmektedir. Dolayısıyla kişisel verilerin korunmasıyla ilgili olarak bilgi güvenliği sağladıkları iddia edilemez. Bu nedenle, belge yönetimi ve arşivcilik prensiplerinin kişisel verilerin güvenliğini de sağlaması için bilgi güvenliği ilkelerine ihtiyaç duymaktadır. Belge yöneticilerine, arşivcilere ve onay mercilerine ait kişisel veriler tehditlerin hedefinde görülmeyebilir. Ayrıca insanların endişelenmesi için düşmanlarının olmasına da gerek yoktur. Ancak bilginin İnternet'teki ticarete konu olan para birimi olduğu unutulmamalıdır. Bilgi kurumlarındaki kişisel veriler düşünüldüğünden daha fazla şey söylemektedir ve oluşturulan içerik değer verilmesini gerektirmektedir ("What is metadata", 2017).

Belge yönetiminde, belgenin kaynağı ve ilgili olduğu tüm bilgi varlıklarına ulaşmanın kolay bir yolu provenansa uygun olarak yapılan arşivsel düzenleme ve arşivsel düzenlemeyi yansıtan üstverilerdir. Bütünlük sağladığı gibi kullanılabilirliği de kolaylaştırmaktadır. Ayrıca, gerektiğinde delil niteliği taşıyan belgenin hem kaynağı hem de bütünlüğü açısından adli bilişimce kullanılmaktadır. Provenans ve üstveri belge yönetimi için büyük öneme haizdir. Çünkü üstveri alanında bir belgenin yetkili otoritece ne zaman imzalandığı tarih bilgisi, zaman

damgası marifetiyle yer alır. Bir belgenin esas tarihi zaman damgasındaki tarih bilgisine dayanmaktadır (Resmi Yazışmalarda Uygulanacak, 2020, s. 5). Belge yönetimi ve arşiv uygulamaları, bütünlük ve kullanılabilirlik ilkelerini bu noktalardan desteklemektedir.

Bilgi güvenliği yaklaşımının kapsamı her iki disiplinin ilkelerini de yansıtmalıdır. Bilgi güvenliği ilkeleri, güvenlik hedeflerini somutlaştırmaktadır. Belge yönetimi ve arşivcilik prensipleri de bu somut hedefleri desteklemektedir.

Kaynakça

Anderson, K. A. (2012). A case for a partnership between information security and records information management. *ISACA Journal, 12*(2), 40-44. https://www.isacajournal-digital.org/isacajournal/2012vol2?pg=46#pg46

Association for Information and Image Management International (AIIM). (2009). *Recommended practice: Analysis, selection, and implementation of electronic document management systems (EDMS).* AIIM International.

Başbakanlık Genelgesi. (2008, 16 Temmuz). *Resmi Gazete* (Sayı: 26938). https://www.resmigazete.gov.tr/eskiler/2008/07/20080716-7.htm

Blanding, S. F. (2004). An introduction to LAN/WAN security. H.F. Tipton ve M. Krause (Ed.) *Information security management handbook* (5. bs.) içinde. Auerbach Publications. http://index-of.co.uk/Computer-Security/CRC%20Press%20%20Information%20Security%20Management%20Handbook,%20Fifth%20.pdf

Brooks, R. (2019, March 26). What is the CIA triad? https://blog.netwrix.com/2019/03/26/the-cia-triad-and-its-real-world-application/

Canbek, G. ve Sağıroğlu, Ş. (2006). Bilgi, bilgi güvenliği ve süreçleri üzerine bir inceleme. *Politeknik Dergisi, 9*(3), 165-174. https://dergipark.org.tr/tr/download/article-file/384578

Çakmak T. ve Eroğlu, Ş. (2020). Elektronik arşivlerde dijital koruma ve bilgi güvenliği risk değerlendirmesi. A. Kuzucuoğlu ve Y. Şeşen (Ed.), *Bilgi merkezlerinde risk ve kriz yönetimi* içinde (ss. 51-78). Hiperyayın.

Çiçek, N. (2011). Elektronik belgelerin diplomatik analizi ve arşivsel bağın kurulmasındaki önemi: Türkiye'deki uygulamalar ışığında bir inceleme. *Bilgi Dünyası, 12*(1) 87-104.

Donaldson, D. ve Bell, L. (2019). Security, archivists, and digital collections. *Journal of Archival Organization, 15*(1-2), 1-19. Doi:10.1080/15332748.2019.1609311.

Eroğlu, Ş. ve Külcü, Ö. (2014). TS 13298 çerçevesinde kurumsal bilgi sistemleri ve elektronik belge yönetimi standartlarının değerlendirilmesi: İçişleri Bakanlığı örneği. *Bilgi Dünyası, 15*(2) 327-352.

Fruhlinger, J. (2020, February 10). The CIA triad: Definition, components and examples. https://www.csoonline.com/article/3519908/the-cia-triad-definition-components-and-examples.html

Henttonen, P. (2017). Privacy as an archival problem and a solution. *Archival Science, 17*(3), 285–303. http://dx.doi.org/10.1007/s10502-017-9277-0

International Organization for Standardization (ISO). (2001). *Information and documentation - Records management - Part 1: General* (ISO 15489-1). Cenevre [İsviçre]: Author.

ISO. (2005). *Informatıon security management* (ISO IEC 27001). Cenevre [İsviçre]: Author.

Kandur, H. (2006). *Elektronik belge yönetimi sistem kriterleri referans modeli* (v.2.0). Ankara: Devlet Arşivleri Genel Müdürlüğü.

Karasar, N. (2012). *Bilimsel araştırma yöntemi* (23. bs.). Nobel Akademi Yayıncılık.

Kelley, M. B. (2013). The stuxnet attack on Iran's Nuclear Plant was 'far more dangerous' than previously thought. https://www.businessinsider.com/stuxnet-was-far-more-dangerous-than-previous-thought-2013-11

Külcü, Ö. (2007). Belge yönetiminin değişen yüzü: Standartlaşma çalışmaları ve uluslararası uygulamalar. *Bilgi Dünyası 8*(2), 230-279. https://bd.org.tr/index.php/bd/article/view/341/338

Lomas, E. (2010). Information governance: Information security and access within a UK context. *Records Management Journa*l, *20*(2), 182–198. https://doi.org/10.1108/09565691011064322

Mansfield-Devine, S. (2015). The Ashley Madison affair. *Network Security*, *9*, 8-16. https://doi.org/10.1016/S1353-4858(15)30080-5

Miller, B. (2010). CIA triad. http://blog.electricfork.com/2010/03/cia-triad.html

Morris Worm. (2022, 4 Şubat). *Wikipedi* içinde. https://en.wikipedia.org/wiki/Morris_worm

Munier, M., Lalanne, V., Ardoy, P.Y. ve Ricarde, M. (2020). *Legal issues about metadata: Data privacy vs information security* [Konferans oturumu]. Proceedings of the 8th International Workshop on Data Privacy Management (DPM'2013) (ss. 162-177) içinde, Sep 2013, Egham, United Kingdom. https://hal.archives-ouvertes.fr/hal-01082056/document

Neuman, W. L. (2008). *Toplumsal araştırma yöntemleri: Nicel ve nitel yaklaşımlar* (Cilt 1, S. Özge, Çev.). Yayın Odası.

Nieles, M., Dempsey, K. ve Pillitteri, V.Y. (2017). An introduction to information security. *NIST Special Publication 800-12* (Revision 1). https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-12r1.pdf

NSW Government State Archives and Records. (2019). *How records and information management techniques and skills can contribute to information security objectives.* https://www.records.nsw.gov.au/recordkeeping/advice/records-management-techniques-and-information-security-objectives

Orange Book (2021). *Computer security - A brief look* içinde. https://sites.google.com/site/cacsolin/orange-book.

Önaçan, M. B. K., Medeni, T.D. ve Özkanlı, Ö. (2012). Elektronik belge yönetim sistemi (EBYS)'nin faydaları ve kurum bünyesinde EBYS yapılandırmaya yönelik bir yol haritası. *Sayıştay Dergisi,* 85.

Öztemiz, S. ve Yılmaz, B. (2013). Bilgi merkezlerinde bilgi güvenliği farkındalığı: Ankara'daki üniversite kütüphaneleri örneği. *Bilgi Dünyası, 14*(1), 87-100. https://bd.org.tr/index.php/bd/article/view/136/130

Pepitone, J. (2014, January 12). TJX: 94 million. https://money.cnn.com/gallery/technology/security/2013/12/19/biggest-credit-card-hacks/3.html

Resmi Yazışmalarda Uygulanacak Usul ve Esaslar Hakkında Yönetmelik. (2020, 10 Haziran). *Resmi Gazete* (Sayı: 31151). https://www.resmigazete.gov.tr/eskiler/2020/06/20200610-8.pdf

Riley, M., Lawrence, D. and Matlack, C. (2014, March 17). Missed alarms and 40 million stolen credit card numbers: How target blew it. https://www.bloomberg.com/news/articles/2014-03-13/target-missed-warnings-in-epic-hack-of-credit-card-data

Schellenberg, T.R. (1951). *Principles of arrangement.* Staff Information Paper Number 18, Published by the National Archives and Records Administration. https://www.archives.gov/research/alic/reference/archives-resources/principles-of-arrangement.html

Seferoğlu, S. S., Yıldız-Durak, H., Karaoğlan-Yılmaz, G. ve Yılmaz, R. (2018). Bilgi güvenliği farkındalığı ve bilgi güvenliği politikalarıyla ilgili bir inceleme. B. Akkoyunlu, A. İşman ve H. F.

Odabaşı (Ed). *Eğitim teknolojileri okumaları* (3. Bölüm, ss. 29-43) içinde. TOJET ve Sakarya Üniversitesi.

Shaw, A. ve Shaw, D.T. (2006). *Electronic records management criteria and information security* [Konferans oturumu]. Proceedings of the 7th Australian information warfare and security conference (ss. 137-144) içinde. Perth Western: Edith Cowan University. http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.163.698&rep=rep1&type=pdf

Stallings, W. ve Brown, L. (2015). *Computer security: Principles and practice* (3. bs.). Pearson Education, Inc.

Stephens, D. O. (2001). Megatrends in international records management. *Information Management Journal*, *35*(4), 66-70.

The Government of Hong Kong Special Administrative Region Government Records Service. (2020). *Guidelines for mManaging records in a hybrid environment.* https://www.grs.gov.hk/pdf/Guidelines_for_Managing_Records_in_a_Hybrid_Environment(Eng_only).pdf

Türk Standardları Enstitüsü (TSE). (2009). *Bilgi ve dokümantasyon-Elektronik belge yönetimi* (TS 13298). Ankara: Yazar.

TSE. (2014). *Elektronik doküman ve belge yönetim sistemi koruma profili* (sürüm1.3.1). Ankara: Yazar. https://statik.tse.org.tr/upload/tr/dosya/icerikyonetimi/2231/09012015111018-3.pdf

TSE. (2015). *Elektronik belge ve arşiv yönetimi sistemi* (TS 13298). Ankara: Yazar.

TSE. (2019). *Bilgi ve dokümantasyon - Belge yönetimi bölüm 1: Genel* (TS ISO 15489-1). Ankara: Yazar.

TSE. (2021) *Türk Standardı*. https://intweb.tse.org.tr/Standard/Standard/Standard.aspx?081118051115108051104119110104055047105102120088111043113104073098108075120107050114074049048106

Turton, W. ve Mehrotra, K. (2021). Hackers breached Colonial Pipeline using compromised password. https://www.bloomberg.com/news/articles/2021-06-04/hackers-breached-colonial-pipeline-using-compromised-password

U.S. Government Accountability Office. (1996). *Information security: Computer attacks at Department of Defense Pose increasing risks.* https://irp.fas.org/gao/aim96084.htm

What is metadata and what does it reveal? (2017). https://opendatasecurity.co.uk/what-is-metadata-and-what-does-it-reveal/

Yalçınkaya, B. (2015). Elektronik belge yönetimi (EBY) uygulamalarında başarıyı olumsuz etkileyen risk unsurları. *Bilgi ve Belge Araştırmaları Dergisi,* 4, 20-40.

Yıldız, A. (2006). Provenans sisteminin amaçları ve uygulanması. *Arşiv Dünyası,* 8, 7-10. https://dergipark.org.tr/tr/download/article-file/207635

Yılmaz, B. ve Özdemirci, F. (2019). Bilgi güvenliği yönetim sistemi (BGYS) sürecinde bilgi güvenliği temelli EBYS yönetimi. B. Yalçınkaya, M. A. Ünal, B. Yılmaz ve F. Özdemirci, (Ed.), *Bilgi Yönetimi ve Bilgi Güvenliği: eBelge- eArşiv- eDevlet- Bulut BilişimBüyük Veri- Yapay Zekâ* (ss. 45-60) içinde. Ankara Üniversitesi.

Zengerle, P. ve Cassella, M. (2015) Millions more Americans hit by government personnel data hack. https://web.archive.org/web/20170228005352/http://www.reuters.com/article/us-cybersecurity-usa idUSKCN0PJ2M420150709