T.C.

DOKUZ EYLÜL ÜNİVERSİTESİ

SAĞLIK BİLİMLERİ ENSTİTÜSÜ

SAĞLIK KURULUŞLARINDA ÖRGÜT İKLİMİ VE BİLGİ GÜVENLİĞİNİN İLİŞKİSİ

BAŞAK GERÇEKER

SAĞLIKTA KALİTE GELİŞTİRME VE AKREDİTASYON ANABİLİM DALI

YÜKSEK LİSANS TEZİ

İZMİR-2012

TEZ KODU: DEU.HSI.MSc/2009970141

T.C.

DOKUZ EYLÜL ÜNİVERSİTESİ

SAĞLIK BİLİMLERİ ENSTİTÜSÜ

SAĞLIK KURULUŞLARINDA ÖRGÜT İKLİMİ VE BİLGİ GÜVENLİĞİNİN İLİŞKİSİ

SAĞLIKTA KALİTE GELİŞTİRME VE AKREDİTASYON ANABİLİM DALI

YÜKSEK LİSANS TEZİ

BAŞAK GERÇEKER

Danışman Öğretim Üyesi: Doç. Dr. Özlem İPEKGİL DOĞAN

İkinci Danışman Öğretim Üyesi: Doç. Dr. Şeyda SEREN İNTEPELER

TEZ KODU: DEU.HSI.MSc-2009970141

Dokuz Eylül Üniversitesi Sağlık Bilimleri Enstitüsü Sağlıkta Kalite Geliştirme ve Akreditasyon Anabilim Dalı Yüksek Lisans programı öğrencisi Başak GERÇEKER tarafından hazırlanan **"SAĞLIK KURULUŞLARINDA ÖRGÜT İKLİMİ VE BİLGİ GÜVENLİĞİ İLİŞKİSİ"** konulu Yüksek Lisans tezini 21/11/2012 tarihinde başarılı olarak tamamlamıştır.

BAŞKAN

Doç. Dr. Özlem İPEKGİL DOĞAN

Prof. Dr. Hüseyin BASKIN

ÜYE

Yrd. Doç. Dr. Bahattin TAYLAN

ÜYE

Yrd. Doç. Dr. Mert TOPAYAN

Y. ÜYE

Doç. Dr. Tonay İNCEBOZ

Y. ÜYE

İÇİNDEKİLER

TABLOLAR DİZİNİ

ŞEKİLLER DİZİNİ

KISALTMALAR

BGYS……Bilgi Güvenliği Yönetim Sistemi

BİT……Bilgi ve İletişim Teknolojileri

BM…….Birleşmiş Milletler

BS……..British Standards

BSI…….British Standards Institue

BT……..Bilgi Teknolojileri

CSI…….Computer Crime & Security Survey

FCC……Federal İletişim Komisyonu

FTC……Federal Ticaret Komisyonu

ICN……International Council of Nurses

IEC……The Internatıonal Electrotchnical Organization

ISO……International Organization of Standardization

JTC…….Joint Technical Committee

PUKÖ……Planla-Uygula- Kontrol Et- Önlem Al

SPSS……..Statistical Programme for Social Sciencies

TS……..Türk Standartları

TSE……Türk Standartlar Enstitüsü

WHO…….Dünya Sağlık Örgütü

SAĞLIK KURULUŞLARINDA ÖRGÜT İKLİMİ VE BİLGİ GÜVENLİĞİNİN İLİŞKİSİ

BAŞAK GERÇEKER
Dokuz Eylül Üniversitesi
Sağlık Bilimler Enstitüsü
Sağlıkta Kalite Geliştirme ve Akreditasyon Anabilim Dalı
Sağlıkta Kalite Geliştirme ve Akreditasyon

ÖZET

Günümüzde küreselleşme sonucu ortaya çıkan teknolojik gelişmeler, yoğun rekabet ve benzeri nedenlerle işletmeler, hayatta kalabilmek ve diğer işletmelerle etkili bir şekilde rekabet edebilmeleri açısından yeni yönetim arayışı içine girmişlerdir. Örgütsel iklimde günümüzde önemini arttırarak yaygınlığını devam ettiren bir yönetim anlayışıdır. İşletmelerdeki örgütsel iklimin ölçülmesi ve değerlendirilmesi, sağlık sektöründe daha başarılı sonuçlar elde etmelerini sağlayacaktır. Bu çalışmanın amacı; son zamanlarda güncel olan bilgi güvenliğinin sağlık sektöründe örgüt iklimi ilişkisini ortaya çıkarmak, sağlık sektöründe örgüt ikliminin önemini vurgulamak, bilgi güvenliği oluşumunda örgüt iklimi ne kadar önemli bir etkiye sahip olduğu belirtmek ve ölçmektir.

Araştırmada literatürden elde edilen bilgiler ışığında oluşturulan yapılandırılmış anket tekniği kullanımıştır. Anket Robert Stringer tarafından geliştirilmiş örgüt iklimi ölçeği ve TS ISO 27799'dan çıkarılan bilgi güvenliği sorularından oluşmaktadır. Çalışma İzmir merkezde toplam 13 hastanedeki yöneticilere uygulanmıştır. Araştırma verileri SPSS 17.0 (Statistical Programme for Social Sciencies) programı ile analiz edilmiştir.

Elde edilen bulgularda, "Bilgi Güvenliğini Organizasyon" yapısının etkilediği ortaya çıkmıştır. "Örgüt İklimi" değişkeni ile "Bilgi Güvenliği" değişkeni arasında pozitif yönde güçlü kuvvette bir ilişki" ($p<0,001$ ve $r= 0,509$) vardır. "Örgüt İklimi"ni etkileyen bilgi yönetimi değişkeni "Bilgi Güvenliği Yönetimi" ($p<0,001$ ve $\beta= ,561$) olarak belirlenmiştir. Bu değişkenler örgüt iklimi ile ilgili çalışanların görüşlerini %32 oranında açıklamaktadır ($R^2=,315$).

Anahtar Sözcükler: Bilgi Güvenliği, Örgüt iklimi, ISO 27799

THE RELATIONSHIP BETWEEN ORGANIZATIONAL CLIMATE AND INFORMATION SECURITY IN HEALTH INSTITUTIONS

BAŞAK GERÇEKER

Dokuz Eylül Üniversitesi

Sağlık Bilimler Enstitüsü

Sağlıkta Kalite Geliştirme ve Akreditasyon Anabilim Dalı

Sağlıkta Kalite Geliştirme ve Akreditasyon

ABSTRACT

Nowadays, the enterprises have sought for a new management in order to survive and compete effectively with other enterprises due to technological developments depending on globalization and competitive practices and similar reasons. Organizational climate is a kind of management concept which has enhanced its importance and sustained its prevalence recently.Measuring and assessing the organizational climate in enterprises will lead to obtain more successful results in health institutions.The aim of this study is to find out the relationship between organizational climate and current information security in health sector,to emphasize the significance of organizational climate in this sector and to define and measure how important effect the organizational climate has in forming the information security.

In the study, structural survey method was used by obtaining information from literature.The questionnaire was composed of information security questions from organizational climate scale and TS ISO 27799 which was developed by Robert Stringer. The study was applied on the managers of 13 hospitals in the centre of İzmir. The data of the research were analyzed by SPSS 17.0 programme(Statistical Programme for Social Sciencies)

In the findings obtained, it was observed that the organizational structure affected information security. Thus, there is a positive and strong relation between ‘organizational climate’ variable and ‘information security’ variable($p<0,001$ and $r= 0,509$) .It was determined that information management variable affecting ‘Organizational Climate’ was defined as ‘Information Security Management’ ($p<0,001$ ve $\beta= ,561$). These variables accounts for %32 of the opinions of those studying related to organizational climate. ($R^2=,315$).

Key Words: Information Security, Organizational Climate, ISO 27799

1. GİRİŞ VE AMAÇ

1.1. Problemin Tanımı ve Önemi:

Örgütsel iklim: örgüte kimliğini kazandıran, örgütte çalışan bireylerin davranışlarını etkileyen ve onlar tarafından algılanan, örgüte egemen olan tüm özellikler serisidir. Başka bir deyişle örgütsel iklim, bireylerin işletme içindeki çalışmanın nasıl olması gerektiğine dair beklentileriyle, bu beklentilerin ne ölçüde gerçekleştiğine dair algılarının sonunda oluşan genel bir kavramdır. Örgütsel iklim, rekabet olgusunun oldukça yoğun bir şekilde yaşandığı günümüz işletmelerinde vasıflı çalışanları bünyelerinde tutabilmeleri için vazgeçilmez bir kavram olarak karşımıza çıkmaktadır. Küreselleşme sonucu ortaya çıkan yeniden yapılanma, yoğun rekabet ve küçülme gibi günümüzde işletmelerin etkilendiği faktörler örgütsel iklim ile doğrudan bir ilişki içindedir (Hocaniyazov, 2008).

Bir örgütte çalışan personelin kurumun amaçlarını benimsemesi, değer yargılarını kabullenmesi, inanç ve normlara uygun ilişkilerde bulunması ve beklenen davranışları göstermesi örgüt iklimi kapsamındadır. Bir örgütü diğerlerinden ayıran ve çalışanların davranışlarını etkileyen iç özellikler dizisi, örgüt iklimi olarak tanımlanmaktadır. Örgüt iklimi, sosyal bir sistemin örgütsel ve bireysel boyutlarını dengelemeye çalışan grubun (çalışan ve yönetici) oluşturduğu bir sonuçtur. Bu sonuç paylaşılan değerleri, sosyal inançları ve sosyal standartları kapsamaktadır (Aytaç, 2003).

Örgüt iklimi / kurumsal iklim, bireysel ve örgütsel düzeyler arasında çözümlemelere olanak veren kavramsal bir bağdır. Örgüt iklimi iş çevresinin, bu çevre içinde yaşayan ve çalışanlar tarafından doğrudan ya da dolaylı olarak algılanan ve onların motivasyonları ile davranışlarını etkileyebileceği varsayılan ölçülebilir bir özellikler kümesidir. Örgüt ikliminin anlaşılması yönetim sürecinin incelenmesinde, değişik yönetim biçimlerinin, örgütte çalışan kişiler, örgütün başardığı iş ve örgüt sağlığı üzerindeki etkisinin anlaşılmasına yardımcı olacaktır (Lim, 2006).

Bilgi yönetimi günümüzün giderek artan rekabetçi ortamına bağlı olarak önem kazanan bir kavramdır. İşgücü ve sermaye yoğun firmaların yerini bilgi yoğun firmaların alması ile birlikte işgücü, makine ve malzeme dışında "bilgi" kavramının tanımlanması ve ön planda tutulması, bilgi süreçlerinin nasıl yönetilebileceği konusunu gündeme getirmektedir. Bilgi yönetimi,

entelektüel sermayenin yönetilmesinden öte, bilginin oluşturulması, dönüştürülmesi ve kullanılması gibi bilgi ile ilgili bütün faaliyetleri de kapsamaktadır. Bilgi yönetiminin işlerlik kazanabilmesi için öncelikle bilgi yönetiminin var olabileceği, gelişebileceği bir ortamın sağlanması gerekir. Bilgi yönetimine yönelik bu alt yapıyı oluşturan başlıca unsurlar örgüt yapısı ve örgüt kültürüdür. Örgütlerde bilgi yönetiminin uygulanması için örgütün bilgiyi elde edip örgüt içinde yayılımını sağlayacak yapıya ve kültüre sahip olması gerekmektedir Örgüt, bilgi yönetimi için gerekli altyapıyı oluşturduktan sonra bu yapı bilgi yönetiminin süreçlerini de etkileyecektir. Bilgi yönetiminde temel süreçler bilgiyi elde etme, elde edilen bilgiyi kullanılabilir bilgiye dönüştürme, elde edilen bilgiyi örgütsel uygulamalarda kullanma ve elde edilen bilgiyi koruma süreçleridir. Örgüt, sahip olduğu kültürü ve örgütsel yapısının etkileri ile bilgiyi elde eder ve bu bilgiyi örgüt içinde yayılacak ve kullanılacak hale getirmeye çalışır. Bilgi yönetiminde örgütü etkinliğe ulaştıracak asıl süreç uygulamadır. Bu nedenle bilgi yönetiminde, bilgiyi elde etmek ve kullanılabilir hale getirmekten ziyade uygulama daha önemli kabul edilir. Bilgiyi koruma süreci ise rekabet üstünlüğü sağlama açısından önem kazanmaktadır. Çünkü taklit edilen bilgiler örgütün tüm kültürel ve yapısal unsurlarını ve bilgi yönetimi süreçlerini rakiplerle paylaşma hatta bunları rakiplere kullandırma anlamı taşır. Bu durum da nihayetinde örgütsel etkinliği olumsuz biçimde etkileyebilir (Gold, 2001).

Sağlık bilişim güvenliği, bilgi üretimi ve bilgi teknolojilerinin yaygın kullanımı ile ciddi boyutlarda artmıştır. Sağlık bilişim teknolojileri kullanımının artması ile bilginin büyük çoğunluğu basılı dokümanlardan, bilgi teknolojileri tarafından işlenir hale dönüşmüştür. Buna paralel olarak sağlık işletmelerinde bilgiye erişim süreci ve hızı oldukça yüksektir. Bu durum, birçok avantajlarının yanı sıra dezavantajı da beraberinde getirmektedir. Sağlık bilgi teknolojileri üzerinde bilinçli veya bilinçsiz yapılan hatalar çok ciddi sonuçlar doğurabilir. Sağlık bilgi teknolojilerindeki açıklıklar ve dikkatsiz yapılandırmalar, bilgiye yetkisiz erişime yol açabilir. Bu durumda sağlıkla ilgili bilginin yetkisiz imhası ve değiştirilmesi söz konusu olabilir. Geçmişte sağlıkta bilgi güvenliği, sadece fiziksel güvenliğin tesis edilmesi ile sağlanırken, günümüzde kurumların en çok zorlandıkları öncelikli bir gereksinim gösteren konulardan biridir.

Sağlık işletmelerinde kurumsal bilgi güvenliği çalışmaları, hizmetin karakteristik özellikleri nedeni ile hizmet sektöründe yer alan diğer isletmelere göre daha farklı yaklaşımlar içerisinde sürdürülmektedir (Marşap, 2010).

1.2. Araştırmanın Amacı:

Günümüzde küreselleşme sonucu ortaya çıkan teknolojik gelişmeler, yoğun rekabet ve benzeri nedenlerle işletmeler, hayatta kalabilmek ve diğer işletmelerle etkili bir şekilde rekabet edebilmeleri açısından yeni yönetim arayışı içine girmişlerdir. Örgütsel iklimde günümüzde önemini artırarak yaygınlığını devam ettiren bir yönetim anlayışıdır. Bu çalışmanın amacı; son zamanlarda güncel olan bilgi güvenliğinin sağlık sektöründe örgüt iklimi ilişkisini ortaya çıkarmak, sağlık sektöründe örgüt ikliminin önemini vurgulamak, bilgi güvenliğinin örgüt iklimindeki yerini belirlemektir.

Sağlık sektöründe çalışanların mutlu bir şekilde hizmet sunabilmeleri için işletmelerdeki iklim önemli hale gelmiştir. Bu nedenle işletmelerdeki örgütsel iklimin ölçülmesi ve değerlendirilmesi, sağlık sektöründe daha başarılı sonuçlar elde etmelerini sağlayacaktır. Bu çalışmadaki amaç bilgi güvenliği oluşumunda örgüt ikliminin ne kadar önemli bir etkiye sahip olduğu belirtmek ve ölçmektir.

1.3. Araştırmanın Hipotezleri

1.3.1. Sağlık kuruluşlarında çalışan yöneticilerin demografik özelliklerine göre örgüt iklimi değişkenleri arasında istatistiksel olarak anlamlı bir fark var mıdır?

1.3.1.a) Katılımcıların cinsiyetlerine göre örgüt iklimi değişkenlerine verdikleri yanıtlar arasında anlamlı bir farklılık var mıdır?

1.3.1.b) Katılımcıların yaşlarına göre örgüt iklimi değişkenlerine verdikleri yanıtlar arasında anlamlı bir farklılık var mıdır?

1.3.1.c) Katılımcıların eğitim durumlarına göre örgüt iklimi değişkenlerine verdikleri yanıtlar arasında anlamlı bir farklılık var mıdır?

1.3.1.d) Katılımcıların görevlerine göre örgüt iklimi değişkenlerine verdikleri yanıtlar arasında anlamlı bir farklılık var mıdır?

1.3.1.e) Katılımcıların toplam iş tecrübelerine göre örgüt iklimi değişkenlerine verdikleri yanıtlar arasında anlamlı bir farklılık var mıdır?

1.3.1.f) Katılımcıların mevcut işyerinde çalışma sürelerine göre örgüt iklimi değişkenlerine verdikleri yanıtlar arasında anlamlı bir farklılık var mıdır?

1.3.2. Örgüt iklimi değişkenleri arasında anlamlı bir ilişki var mıdır?

1.3.3. Sağlık kuruluşlarında çalışan yöneticilerin demografik özelliklerine göre bilgi güvenliği değişkenleri arasında istatistiksel olarak anlamlı bir fark var mıdır?

1.3.3.a) Katılımcıların cinsiyetlerine göre bilgi güvenliği değişkenlerine verdikleri yanıtlar arasında anlamlı bir farklılık var mıdır?

1.3.3.b) Katılımcıların yaşlarına göre bilgi güvenliği değişkenlerine verdikleri yanıtlar arasında anlamlı bir farklılık var mıdır?

1.3.3.c) Katılımcıların eğitim durumlarına göre bilgi güvenliği değişkenlerine verdikleri yanıtlar arasında anlamlı bir farklılık var mıdır?

1.3.3.d) Katılımcıların görevlerine göre bilgi güvenliği değişkenlerine verdikleri yanıtlar arasında anlamlı bir farklılık var mıdır?

1.3.3.e) Katılımcıların toplam iş tecrübelerine göre bilgi güvenliği değişkenlerine verdikleri yanıtlar arasında anlamlı bir farklılık var mıdır?

1.3.3.f) Katılımcıların mevcut işyerinde çalışma sürelerine göre bilgi güvenliği değişkenlerine verdikleri yanıtlar arasında anlamlı bir farklılık var mıdır?

1.3.4. Bilgi güvenliği değişkenleri arasında anlamlı bir ilişki var mıdır?

1.3.5. Örgüt iklimi ve bilgi güvenliği arasında anlamlı bir ilişki var mıdır?

2. GENEL BİLGİLER

2.1.ÖRGÜT İKLİMİNDE TEMEL KAVRAMLAR

2.1.1.Örgüt İklimi

İklim: kelime anlamı olarak atmosfer, hava anlamındadır. Etimolojik yönden iklim (climate) sözcüğü Yunancadan gelmektedir ve eğilim anlamını taşır. Bu sözcük yalnız ısı ve basınç gibi fiziksel olayları anlatmaz, aynı zamanda örgüt üyelerinden birinin iç çevreyi nasıl tanımladığını da anlatır. İnsanların, tutum ve davranışlarını tahmin etmemize yardımcı olan kalıcı ve sabit özellikleri olduğu gibi, örgütlerin de insanlar gibi katı, dost, sıcak, yenilikçi ya da tutucu gibi terimlerle ifade edilebilir özellikleri vardır. Bu özellikler seti örgütün psikolojik yanını oluşturur.

İklim, hava, ortam, atmosfer, ahlak, kişilik gibi kavramlar örgütler açısından 1960'lı yıllardan itibaren oldukça ilgi gören konulardır. Örgüt kültürü kavramının popüler hale gelmesiyle birlikte bu konular örgüt kültürüyle birlikte ele alınmaya başlamıştır. İklim, yönetimde insan ilişkileri yaklaşımıyla birlikte gündeme gelmiş, 1960 ve 1970'li yıllarda oldukça ilgi görmüştür. Bu konudaki ilk çalışmalardan biri Halpin'in çalışmasıdır. K.Levin, C. Barnard, P. Selznick gibi yönetim bilimciler de 1930 ve 1940'lı yıllarda örgütlerin psikolojik, kültürel, sembolik yönüne dikkati çeken ilk araştırmacılardır. Örgüt iklimi çalışmaları davranışı insan ve çevrenin bir fonksiyonu olarak gören K.Lewin'in "Alan Teorisine" ve sosyal psikoloji bakış açısına dayandırılmakta ve çevre değişkenlerini açıklamaya odaklanmaktadır. Örgüt iklimi araştırmalarının temelindeki varsayım, örgütsel iklim yönünden örgütler arasında bazı farklılıkların olabileceği ve bu farklılıkların da örgütsel etkililiği etkilediği şeklinde olmuştur (Aydoğan, 2004; Şişman, 2002). 1968'de Litwin ve Stringer'in "motivasyon ve örgüt iklimi" konusunda birlikte yaptıkları çalışmalarla başlamış ve Tiguiri ve Litwin'in "örgüt iklimi kavramı" başlıklı eserleriyle devam etmiştir. Litwin ve Stringer iklimin kendisinin, önceki davranış eğilimlerini elde etmekten daha güçlü olduğunu kanıtlamışlardır. Bunun sonucunda da iklimin grup üyelerinin örnek bir davranışla değişebileceğinin farkına varmışlardır. Bu da liderlik davranışlarıyla olabilmektedir. Son olarak da değişik liderlik çeşitlerinin ortaya çıkmasına sebep olmuştur (Özdere, 2010).

Örgüt ikliminin ilk tanımlarından birini yapan Forehand ve Gilmer örgüt iklimini, 'örgütü tanımlayan ve örgütü diğer örgütlerden ayıran, zaman içinde oldukça sürekli ve değişmez olan, örgütteki bireylerin davranışlarını etkileyen özellikler setidir' şeklinde tanımlamışlardır (Karcıoğlu, 2001).

Bir örgüt açısından örgütsel iklim ise, o örgütteki mevcut koşulların çalışanlar tarafından algılanış biçimini ve örgütsel yaşamın niteliğini ifade etmektedir. Örgütsel iklim personelin iş çevresini nasıl yorumladığıdır (Smith, 2008).

Katz ve Kahn göre örgüt iklimi, bir örgütle ilgili olarak psikolojik açıdan tanımlanan ve örgütteki insan ilişkilerinin niteliğini ifade eden bir kavramdır. Yani örgütün psikolojik ortamına örgüt iklimi denir (Özdere, 2010).

ICN (2007) örgüt iklimini, 'çalışanların çalışma ortamlarıyla ilgili paylaştıkları algılardır' şeklinde tanımlamıştır. Siu (2002) örgüt iklimini, 'resmi ve resmi olmayan örgütsel politikaların, uygulamaların, süreçlerin, örgütün belirttiği amaçların ve bu amaçlara ulaşmada uygun anlamların paylaşılan algılamaları' olarak tanımlamıştır. Örgüt iklimi; endüstri ve örgüt psikolojisi, örgütsel davranış ve yönetim bilimleri alanında yapılan pek çok araştırmaya konu olan önemli bir kavramdır. Konunun çalışan açısından önemi, örgüt ikliminin çalışanların işe dayalı duygu, tutum ve davranışlarını etkilemesidir. Aynı zamanda bir örgütte egemen olan iklimin anlaşılması, çalışma ortamıyla ilgili konuları tanımlamak ve anlamak bakımından oldukça yararlıdır (Şişman, 2007).

Örgütsel iklim başlangıçta belirli bir zaman dilimi içerisinde süregelen örgütü açıklayıcı özellikler seti olarak tanımlanmıştır. Bu tanıma göre örgütü diğer bir örgütten ayıran ve o örgütteki insan davranışlarını etkileyen özelliklerin başlıcalar büyüklük, yapı, karmaşıklık, liderlik tarzı ve amaçların yönüdür (Yüksel, 2003).

Örgütsel iklim, tanımlanması zor bir kavramdır. Çevresel güçlerin birleşmesinden meydana gelen coğrafi bölgeler iklimine ya da hava tanımlamalarına benzetilebilir. Bu çerçeve örgüte uyarlandığında, örgütü çevreleyen yaygın atmosfer, moral düzeyi, örgüt üyeleri arasında iyi niyet, ait olma duygusunun gücü şeklinde ifade edilebilir. İklim, örgüte yönelik işgören algılarının temeline dayanır (Terzi, 2000). Örgüt iklimi en geniş tanımıyla çalışma çevresi ile ilgili bir dizi özellik anlamındadır (Arslan, 2004).

Örgüt iklimi; örgütün kişiliğini oluşturan, örgütü diğer örgütlerden ayıran örgütü tanımlayan, örgüte egemen olan ve örgütte bulunan bireylerin davranışlarını etkileyen ve onlardan etkilenen, somut olarak gözle görülen elle tutulamayan, ancak örgüt içindeki bireylerce hissedilen, algılanabilen ve bütün bu özellikleri içine alan psikolojik bir kavramdır (Arslan, 2004; Özdemir, 2006; Şişman, 2002).

Örgütsel iklim, birey üzerine odaklanan ve kavrama süreci ve davranışı anlama konusuna eğilen, psikolojik bir yaklaşım olarak kavramsallaştırılır. Örgütsel iklim, psikolojik yöne dikkat çeker, bireylerin davranışlarını ön alana alır. Çalışmalar, örgütsel üyelerin yakın deneyimleri yerine bireysel kavramlara odaklanır. Tutumsal tepkiler ya da bu deneyimlerin anlayışları anketlerdeki maddelerle ölçülür. Böylece bireylerin bir grup insan tarafından paylaşılan inanç, değer ya da normları yerine bireylerin örgüt hakkında anlayışlarını ölçmeye odaklanmış olur (Çetin, 2004). Örgüt iklimi yöneticiler ve çalışanlar tarafından farklı biçimlerde algılanabilir. Önemli olan iklimin çalışanların bireysel, yöneticilerin yönetimsel amaçlarıyla paralellik göstermesidir. Bir örgütün amaçları doğrultusunda başarıya ulaşabilmesi için örgüt üyelerinin örgüte bakış açılarının pozitif olması, örgüt kültürüne sahip çıkmaları, pozitif bir örgüt iklimine sahip olması gerekmektedir, aksi durumda olumsuz iklimden söz etme olasılığı artacaktır (Küçükgöde, 2005).

Örgüt iklimi, iş görenlerin çevreyi nasıl algıladıklarıdır. Bu algılar, iş görenlerin çevreyi nasıl anlattıkları ve hoşlanıp, hoşlanmadıkları şeylerdir. İklim, örgütün özel niteliklerinin bütünüdür (Tarı, 2002).

Payne, R.L. ve Mansfield, R, örgüt ikliminin farklı yönleri ile örgütsel yapı, çevre ve hiyerarşik pozisyon arasındaki beklenen iliksiyi incelemişlerdir. Örgüt ikliminin önemli ölçüde örgütün büyüklüğünden ve bağımlılığından etkilendiğini tespit etmişlerdir. Ayrıca örgüt iklimi algılamasında hiyerarşik seviyenin etkisinin incelenmesi seviyeye göre önemli değişiklikler göstermiştir. Örgütsel hiyerarşide üst düzey görevliler örgütlerini daha az otoriter, işe dönük, daha arkadaşça ve yeni fikirlere daha açık olarak algılamaktadırlar (Özdere, 2010).

Reichers ve Schneider, örgüt iklimi kavramını, örgütsel politika, uygulama ve süreçlerle ilgili hem formal, hem de informal nitelikte bir ortak algılama olarak tanımlamaktadır. Aynı zamanda örgüt iklimini, kavram olarak örgütün genel görünümünün başta gelen unsuru olarak saymışlardır (Özdere, 2010).

Zeffane'ye göre çalışanların örgüte bağlılığını, heyecanını ve moralini yükseltmek için sadece güdümleyici unsurları çalışanlara sunmak yeterli değildir. Örgütte bulunan olumsuz unsurları ortadan kaldırmak gereklidir. Aynı zamanda, yönetim sisteminde var olan olumsuz unsurları da ortadan kaldırmak gerekmektedir. Benzer düşünce, örgüt iklimini biçimlendirme çalışmalarında da geçerlidir. Yani örgüt ikliminde var olan ve çalışanların motivasyonunu engelleyen unsurlar düzeltilerek, önemli proje ve programların başarı şansı artırılabilir (Özdere, 2010).

Adler ve Borys'a (1996) göre, yöneticiler çalışanlara destek vererek, yenilikçilik, yaratıcılık ve bürokrasi gibi örgüt iklimi boyutlarını analiz ederek, örgütsel stratejilerinin etkinliğini artırabilirler. Özellikle de, çalışanların örgütün amaçlarını gerçekleştirmelerini isteyen, faaliyetlerine katılımını ve sorunların çözümüne katkı sağlamalarını isteyen yöneticiler, örgüt iklimini farklı boyutlardan değerlendirip anlamalıdırlar. Adler ve Borys örgüt ikliminin, planlama ve strateji geliştirme faaliyetlerini daha da başarılı hale getirdiğini savunmaktadırlar (Özdere, 2010).

2.1.2.Örgüt İkliminin Önemi

İklim bütün örgütsel ve psikolojik faaliyetleri (iletişim, problem çözümü, çelişki çözümü, eğitim, motivasyon v.b.) etkiler, örgütün verimliliği ve iş tatmini üzerinde doğrudan ciddi bir rol oynar. Örgütteki birey iklimden doğrudan etkilenir. Bireyin davranışları üzerindeki en büyük etkiyi yaratan da bu iklim şartlarıdır. Örgüt iklimi aynı zamanda örgütün bir sosyal sistem olarak tanımlanmasında ve üyelerin psikolojik ödüllendirme sistemlerinde de rol oynar. Örgütü oluşturan bireyler arasındaki karşılıklı güven ve anlayış ortamı olarak görülebilir.

Örgütsel iklim üyelerin moral seviyesini, bireysel ilişkilerindeki tahammül sınırlarını ve iş performanslarını doğrudan etkileyecektir. Ancak moral de objektif olarak ölçülmesi zor bir kavramdır. Örgüt iklimi üyeler arasında bir işbirliği ruhu yaratmadıkça, onları nitelikli ve verimli çalışmaya motive etmedikçe, örgütün optimum iş performansı elde etmesi olası değildir.

Örgütsel işlevlerin sağlıklı bir biçimde yürütülmesine ek olarak yönetimin personelin istekli ve verimli çalışmasını motive edici bir örgüt iklimini de oluşturması gerekir. Sağlıklı bir örgüt iklimi tek başına örgütsel etkinliği garanti edemez. Ancak örgüt iklimi üyeler arasında, yüksek moral ve motivasyon, iş görenlerdeki örgütü benimseme ve sahip çıkma ruhunu uyandırma en

önemli faktörlerdir. Bu benimseme ve ait olma ruhu, iş görenlerin iş performanslarının etkinliğinde başrolü oynar.

İklim aynı zamanda liderlik davranışlarını doğrudan etkiler. Huzur ve başarı ortamı doğuran bir örgüt iklimi, lideri daha az otoriter ve daha çok hoşgörülü olmaya yöneltir. Bir kriz iklimi ise gerginliğe sebep olur ve liderleri daha sert, merkezi ve otoriter olmaya yönlendirir.

Bir bütün olarak örgütte iklim, girdilerle çıktılar arasında ciddi rol oynayan bir değişken olarak öne çıkmaktadır. İklim örgütsel ve psikolojik olarak işlevleri etkilemekte ve örgütsel işlevlerin sonuçlarında ciddi bir etki yaratmaktadır. Yani iklim örgütün üretim, kar, iş tatmini gibi çıktıları üzerinde belirleyici bir rol oynamaktadır. Örgüt iklimi çalışanların başarısını ve tatminini etkileyeceğinden örgütsel amaçlara ulaşmada örgüt ikliminin geliştirilmesinden yararlanılabilir (Demirel,1997).

2.1.3.Örgüt İkliminin Boyutları

Örgüte kişilik veren, örgüt üyelerini etkileyen ve örgüt üyelerinin her biri tarafından farklı biçimlerde algılanan örgüt ikliminin boyutlarının neler olduğu konusunda da farklı görüşler bulunmaktadır. Örgüt iklimi boyutları söyle gruplamak mümkündür:

Bireysel Özellikler: Doyum, yükselme ve ilerleme olanakları, kişiye verilen önem ve saygınlık, engelleme, güven duygusu, öteki örgüt üyelerine karşı beslenen duyarlılık, tehlikeyi göze alabilme, arkadaşlık ilişkileri.

Örgütsel Özellikler: Örgüt yapısı, örgüt politikası, örgütün amacı, büyüklüğü, ödül düzeni ve ücret, örgütsel çatışma, örgütle bağdaşmazlık çok sıkı gözetim ve denetim, iletişim, önderlik, karar verme, örgütün gelişme olanakları, örgütsel açıklık, sorumluluk.

Çevresel Özellikler: Sınırlayıcı ve güdeleyici çevre, çalışma koşulları (Sıkıcı, Hoşnut edici), yönetsel destek, baskı, uyum, yönetimi eleştirme (Bucak, 2002).

1968'de Litwin ve Stringer, örgütsel iklimle ilgili olarak 8 boyut geliştirmişlerdir (Gürkan, 2006). Koys ve DeCotiis, örgüt iklimini sekiz genel boyut altında toplamıştır. Bunlar Tablo 1'de gösterildiği üzerine; özerklik, işbirliği, güven, baskı, destek, farkedilme, adalet ve yenilikçiliktir.

TABLO 1: Örgütsel İklim Boyutları (Gürkan, 2006)

Örgüt İklimi Ölçeği	**Tanım**
Yapı	Kurallar, düzenlemeler ve resmi prosedürlerle çalışan davranışı üzerindeki kısıtların derecesi
Sorumluluk	Çalışanların işlerini yapmak zorunda oldukları özerkliğin derecesi
Ödül	Ödeme/promosyon ve iş performansı arasındaki ilişkinin derecesi
Risk	İşte ve örgütteki risk alma derecesi
Samimiyet ve Destek	Örgütteki arkadaşça takım ruhunun derecesi
Standartlar	Tam ve açık kişisel ve grup hedefleri ve performans standartlarının algılanan önemi
Çatışma	Problemlerin nasıl çözüleceği hakkındaki farklı fikirleri dinlenme derecesi
Özdeşleşme	Şirkete ait hissetme duygusu

Örgüt iklimi boyutları konusunda araştırma yapan her araştırmacı, farklı boyutlara odaklanarak çalışmalarını yürütmüşlerdir. Bu çalışmada uygulanan ankette Robert Stringer'ın örgüt iklimi ölçeği kullanıldığı için, öncelikle Robert Stringer (2002)'in üzerinde durduğu 6 boyuta değinilecektir.

2.1.3.1. Robert Stringer'e Göre Örgüt İklimi Boyutları

Örgüt iklimi üzerine çalışmaları olan Robert Stringer ise örgüt iklimi boyutlarını altı kategoriye ayırmış ve özet olarak şu sekilde vermiştir (Özdere, 2010):

1. Örgütsel Yapı

Çalışanların, iş ortamındaki resmiyet derecesi ile davranış özgürlüğü ve kısıtlamaları hakkındaki hissettikleridir. Yapı, çalışanların örgütte iyi organize olmalarını ve iyi hissetmelerini sağlamaktadır. Bununla beraber, çalışanların rol ve sorumluluklarını açık bir şekilde tanımlamaktadır. Bir örgütün yapısı eksik olduğu zaman, yetkili karar mercinin kim olduğu ve kimin ne görev yapacağı konusunda tartışma meydana gelmektedir. Çalışanların motivasyon ve performanslarını arttırmada büyük etkisi bulunmaktadır.

2. Standartlar

Performans standartları ile gizli ve açık hedeflerin algılanmasının önemini; iyi bir iş çıkarıldığında yapılan vurguyu; kişisel ve takım hedeflerine ulaşmada gösterilen çabayı gösterir. Standartlar performansı geliştirmek için baskının hassasiyetini ve iyi bir iş yapmakla gururlanan çalışanların derecesini ölçmeye yarar. Yüksek standart ise çalışanların performanslarını geliştirmek için yöntemler aramasını sağlamaktadır. Standartların düşük olması ise performans için düşük beklentileri göstermektedir.

3. Sorumluluk

Önemli bir işi, iyi şekilde yapacağına güvenilme hissidir. Sorumluluk, çalışanların yaptığı işi daha iyi yapmasını, dikkatli bir şekilde planlamasını, olumsuzluklara karşı önlemler almasını, işinin sonuçlarını takip etmesini, ortaya bir olumsuzluk çıktığında bunu üstlenmesini sağlayacaktır. Yüksek sorumluluk hissi, çalışanların kendi problemlerini çözmede cesaretli davranmalarını sağlar. Düşük sorumluluk hissi ise yeni yaklaşımlar karşısında risk almamaya ve test etmemeye yöneltmektedir.

4. Tanıma

Çalışanların, iyi yapılan bir iş için ödüllendirileceği ve takdir göreceği hissidir. Tanıma, eleştiri ve cezaya karşı yerleştirilen vurgunun bir ölçüsüdür. Yüksek tanıma iklimi, ödül ve eleştirinin uygun bir dengesi ile sağlanır. Düşük tanıma iklimi ise işin dengesiz bir şekilde ödüllendirilmiş olduğunu göstermektedir.

5. Destek

Çalışanların ve yöneticilerin karşılıklı yardımlaşma ve desteğinin derecesine yönelik algıdır. Destek yüksek olursa çalışanlar iyi bir takımın parçası olduğunu ve ihtiyaçları olursa özellikle patrondan ya da yöneticilerden yardım alabileceğini hissederler. Eğer destek düşük olursa çalışanlar kendilerini yalnız hissederler.

6. Bağlılık

Çalışanların örgütsel hedefler ile özdeşleştiği, örgütsel üyeliğe değer verdiği ve örgütsel hedefleri elde etmek için sıkı çalışma niyetinde olduğu bir örgüt iklimi boyutudur. Bağlılığın yüksek hissedilmesi kişisel bağlılığın yüksek seviyede olması ile ilgilidir. Bağlılığın düşük seviyede olması ise çalışanların örgüt hedefleri ve örgüte karşı ilgisiz hissettiği anlamına gelmektedir.

2.1.4. Sağlıklı Bir Örgüt İkliminde Bulunan Özellikler

İdeal örgüt tanımlarına tam olarak uyan bir örgüt belki de yeryüzünde yoktur. Ancak güçlü bir örgüt ikliminin var olduğunu söylemek için şu özellikler gerekir (Demirel, 1997):

1. Güven*:* Güven ve emniyet duygularını karşılıklı ve fiilen var olmasını sağlamak için gereken çaba örgütün her kademesindeki personel tarafından gösterilmelidir. Bütün personel güven duyabilecek nitelikte olmalıdır.

2. Katılımcı Karar Alma Mekanizması*:* Örgütün her kademesindeki personel gerek yayımlar yoluyla, gerekse doğrudan sözlü iletişim ile konumları ilgilendiren örgüt politikaları konusunda bilgilendirilmeli. Elemanlar güçlü bir iletişim ağıyla desteklenmeli ve gerektiğinde üstleriyle rahatça koordinasyon kurup karar alma mekanizmalarında ve örgüt hedeflerine yönelik adımlarla söz sahibi olabilmeliler.

3. Destekleme: Örgüt içi ilişkilerde açık sözlülük ilkeleri hakim olmalı. Böylece elemanlar astlarına ve üstlerine karşı kafalarındakileri rahatça söyleyebilmeliler.

4. Aşağıya Doğru İletişimde Açıklık: Özel güvenlik sırları hariç, örgüt üyeleri işleriyle ilgili acil bilgilere kolaylıkla ulaşabilmeliler. Böylece işleriyle, diğer personel ve departmanlarla, yöneticiler ve planlarıyla koordinasyon içinde çalışabilirler.

5. Yukarı Doğru İletişimde Açıklık: Örgütün her kademesindeki personel, astları tarafından yapılan önerileri ve hazırlanan raporları açık yüreklilikle dikkate almalı, astların sunduğu bilgiler dikkatle incelenmelidir.

6. Yüksek Performans Hedeflerine İlgi: Örgütün her kademesindeki personel örgüt hedeflerini (yüksek verimlilik, yüksek kalite, düşük maliyet) benimseyip en az diğer elemanlar kadar çaba göstermelidir (Demirel, 1997).

Örgüt ikliminin sahip olduğu özellikler konusunda aşağıda birkaç yazarın görüşlerine yer verilmiştir.

2.1.4.1. Batlis'e Göre Örgüt İkliminin Özellikleri

Batlis 'e göre örgüt ikliminin genel özellikleri şu şekildedir (Batlis,1980):

- Örgüt iklimini, organizasyon üyelerinin ve özellikle üst yönetimin politika ve davranışları oluşturur,
- Örgütün iş ortamı ile alakalı şartların algılanmasına dayanır,
- İş ortamının yorumlanmasında önemli bir temeldir,

- Örgütteki faaliyetleri yönlendiren baskı kaynağıdır.

2.1.4.2. Al-Shammari'ye Göre Örgüt İkliminin Özellikleri

Al-Shammari (1992) örgüt iklimiyle ilgili makalesinde, örgüt iklimiyle ilgili dört özellikten bahsetmiştir: Bunlardan birincisi; bütün iklimler algısaldır. Bütün iklimler, doğasında algısal ve psikolojik olmayı içerir. İkinci değindiği nokta, bütün iklimlerin soyut olduğudur.Üçüncüsü, iklimler algısal ve soyut olduğu için, diğer psikolojik kavramlar gibi algıların benzer ilkelerinin konusunu kapsayabilirler. Son olarak da, iklimler değerlendirilebilir değil tanımsaldır. Bu yüzden çoğu iklim araştırmacısı, bireylere iş çevrelerinde gördükleri iyi ve kötü şeyleri sormaktan çok sadece ne gördüklerini sorarlar (Al-Shammari, 1992).

2.1.4.3. Mullins'e Göre Örgüt İkliminin Özellikleri

Mullins (1989)'e göre her örgütün kendine özgü özellikleri olsa da, sağlıklı bir örgüt iklimi aşağıdaki özelliklere sahip olmalıdır (Mullins, 1989):

- Örgütsel amaçlar ve kişisel amaçları bütünleştirme,
- Otorite, kontrol ve haberleşme ağı olan ve bireysel üyeler için bağımsızlık içeren esnek bir yapı,
- Farklı koşullar karşısında gösterilen uygun liderlik türleri,
- Örgütün farklı birimleri arasında karşılıklı güven, saygı ve destek,
- Bireysel farklılıklar ve tutumlar ile bireylerin ihtiyaç ve beklentilerini saptama,
- İş tasarımı ve çalışma hayatının kalitesine yönelik ilgi,
- Yüksek performans standardına sahip işleri yerine getirme ve bu standartlara yönelik sorumluluk,
- Ödül, destek, politika ve uygulamalarda adil bir sistem,
- Kişisel gelişim, kariyer sahibi olma ve ilerlemeye yönelik fırsatlar,
- Kişisel ve endüstriyel iliksiler politikaları ve uygulamaları,
- Çatışmaları ertelemeksizin çeliksilerin açıkça tartışılması,
- Örgüt ile birlikte bir kimlik duygusu, örgüte bağlılık ve örgütün önemli bir üyesi olma hissi.

2.1.5. Örgütsel İklim Tipleri

Örgüt ikliminin türleri konusunda aşağıda Halpin ile Litwin ve Stringer'in görüşlerine yer verilmiştir.

2.1.5.1. Halpin'e Göre Örgüt İklimi Türleri

Halpin(1966), örgüt iklimi türlerini 6 kategoride incelemiştir. Bunlar aşağıda kısaca açıklanmıştır (Halpin, 1966):

***1. Açık İklim*:** Örgütteki çalışanların morallerinin çok yüksek olduğu, yönetici ve astlarının uyum içinde çalıştıkları iklim türüdür. Yöneticiler eleştirilere her zaman açıktırlar ve asla kişisel kurallar koymazlar. Tüm görevler büyük bir zevk ve gayretle yapılır. Bu iklimde destekleyici liderlik tarzı görülür.

2 .Bağımsız İklim: Açık iklimle benzer özellikler gösterse de bağımsız iklimi açık iklimden ayıran nokta, bağımsız iklimde açık iklimin tersine yönetici ile astlar arasında psikolojik bir uzaklık, belirli bir mesafe bulunmaktadır.

3. Kontrollü İklim: Kontrollü iklimde görevi yerine getirmek esastır. Üst yönetim tarafından konulmuş olan kuralların dışına pek çıkılmaz. Yöneticilerde benim söylediğim doğrudur, bakısı hâkimdir. Karşılıklı kişisel ilişkiler ve arkadaşlıklar için pek zaman yoktur ve gereksiz çalışmaların varlığı nedeniyle moral oldukça düşüktür.

4. Samimi İklim: Yöneticinin kendisiyle birlikte tüm çalışanları bir aile havasına sokmaya çalıştığı ve sosyal ihtiyaçların tatmininin yüksek olduğu bir iklim tipidir.

5. Babacan İklim: Yöneticinin, astlarını kontrol etmede ve onların sosyal gereksinimlerini karşılamada çabasının yetersiz kaldığı, çalışanların verimli çalışma ve performans gösteremedikleri, çeşitli gruplara ayrıldıklarının görüldüğü, moral düzeyinin düşük olduğu iklim türüdür.

6. Kapalı İklim: Yöneticinin emredici olduğu, işlerin nasıl yapılacağı konusunda kişisel kurallar koyduğu, çalışanları güdülemede yetersiz kaldığı ve tutarsız davranışlar gösterdiği bir iklim türüdür. Moral, samimiyet, işe dönüklük ve anlayış gösterme çok düşüktür. Çalışanlar arası samimi ilişkiler ve arkadaşlık söz konusu değildir. Çalışanların kişisel zenginlikleriyle ilgilenilmez.

2.1.5.2. Litwin ve Stringer'e Göre Örgüt İklimi Türleri

Litwin ve Stringer (1968), yaptıkları deneysel araştırmalarda 3 farklı iklim türünden bahsetmişlerdir. Bunlar :

1. Otoriter Yapılı İklim: Görevlerin kesin tanımı üzerinde duran ve biçimsel otoritenin ödün vermeksizin kullanılmasını ifade eden iklim türüdür. Erke dayalı bir iklimdir. Bu yüzden otoriter yapılı iklim, korku ve başarısızlık beklentisi olan, örgüt dışı siyasal baskının fazla olduğu, görevin ilginç bulunmadığı, çalışanların üstlerine fazla bağımlı olduğu, çalışanları iten, örgüt içi çatışmanın yoğun olduğu, güdülemenin az bulunduğu bir iklim türüdür.

2. Demokratik Yapılı İklim: Birlikte çalışma, gruba bağlılık ve karşılıklı dayanışmanın olduğu, cezalandırmanın olmadığı bir yapıyı ifade eden iklim türüdür.

3. Başarıya Yönelik İklim: Yeniliğin ve örgüt içi rekabetin desteklendiği, başarının hedeflendiği bir yapıyı temsil eden iklim türüdür. Başarıya dayalı bir iklim, güven ve birliktelik duygusunu içeren, örgüt üyelerinin gereksinimlerini karşılayan, özendirici, doyumun fazla olduğu, başarı ve yaratıcılık yeteneklerini kullanmaya yönelten, örgütü benimseme ve bağlılık duygularının yüksek olduğu bir iklim türüdür.

2.I.6.Örgüt İkliminin Sağlık Alanındaki Rolü

Sağlıkla ilgili araştırmaların çoğu, çalışanların daha çok doyum, daha az stres ve tükenmişlik yaşadıkları bir iklimde çalıştıkları zaman destekleyicilik, sorumluluk verici liderlik, olumlu ekip çevresi ile örgütsel uyuma daha fazla sahip olduklarını göstermektedir (Clarke, 2006; Stone etal., 2005). Örgütlerin başarısı büyük oranda, insan unsurunun çok yönlü ve karmaşık yapısının iyi anlaşılmasına ve bu yapıya uygun çalışma ortamının oluşturulmasına bağlıdır.

Çalışma ortamındaki çevresel faktörlerin keşfedilmesi ve geliştirilmesi, personelin daha istekli çalışması ve yüksek performans gösterip üretimi artırmalarına neden olmaktadır.

Yönetim psikolojisi, önceleri bireysel davranışların çevreyi nasıl etkilediği konusu ile ilgilenirken; daha sonraları özellikle de sanayi psikolojisi personel üzerinde çevresel faktörlerin etkisini incelemeye yönelmiştir (Arslan, 2004).

2.1.7. Sağlık Hizmetlerinde Örgüt İklimini Etkileyen Faktörler

Sağlık hizmetlerinde örgüt iklimini etkileyen faktörlerin çok fazla olduğu görülmektedir. Bunlardan bir kısmı;

1. Tepe Yöneticilerin Liderlik Yaklaşımları:

Özel hastanelerde tepe yöneticilerin (yönetim kurulu başkanları) liderlik yaklaşımlarına bağlı olarak astlarının çalıştıkları kurumla ilgili iklim algılamaları etkilenmektedir. Tepe yöneticilerin dönüşümsel liderlik yaklaşımlarının astları tarafından güçlü algılanması sonucunda astların çalıştıkları kurumla ilgili iklim algılamaları daha olumlu ve güçlü bir duruma gelmektedir (Gayef, 2006).

2. İletişim :

Sağlık hizmetlerinde takım çalışmasını etkileyen etmenlerden birisi olan bireyler arası ilişkiler ve iletişimin güçlü olması aynı zamanda yöneticilerin iklim algılamaları üzerinde de etkili unsurlar arasında bulunmaktadır.İletişimin güçlü olduğu kurumlarda üyeler arasında açıklık, karşılıklı anlayış ve güven duygusu yüksektir. Diğer taraftan iletişimde kopuklukları olan kurumlarda güvensizlik, şüphe ve gizlilik bulunmaktadır. Bu tür kurumlarda iklimin algılanması da olumsuz yönde etkilenmektedir (Demirel, 1997).

Sağlık hizmetlerinde çalışan yöneticiler arasında formal ve informal olarak bireyler arası ilişkilerin güçlü olması sonucunda yöneticilerin iklim algılamaları da güçlü olmaktadır.

3.Ödül Sistemleri:

Sağlık hizmetlerinde takım çalışmasını etkileyen etmenlerden birisi olan ödül sistemleri, aynı zamanda iklim üzerinde de etkili olmaktadır. Kullanılan ödül sistemlerinin astların kültürel özelliklerine uygun olması, performansa dayalı olarak kullanılması, adaletli olması ve aynı zamanda çatışmaları en aza indirebilmesi gibi özelliklerin bulunması sonucunda tepe yönetime bağlı çalışan yöneticilerin (astların) iklim algılamaları güçlü olmaktadır. Sağlık hizmetlerinde çalışan yöneticilerin iklim algılamaları üzerinde etkili olan diğer etmenler, politika, kurallar ve prosedürlerin herkesin anlayabileceği ve benimseyebileceği bir düzeyde olması, yöneticilerin kararlara katılma konusunda cesaretlendirilmeleri ve karar verme ile ilgili sorumluluk sahibi olmalarının sağlanması şeklinde özetlenebilir.

Yukarıda açıklanan tepe yöneticilerin liderlik yaklaşımları ve belirtilen diğer faktörlerden örgüt iklimini etkileyen değişkenlerin çok fazla olduğu görülmektedir. Tepe yöneticilerin

dönüşümsel liderlik yaklaşımlarını güçlü olarak algılayan astlarının örgüt iklimi algılamalarının da güçlü olması sonucunda sağlık hizmetlerinde hedeflere ulaşma, olumlu ve verimli çıktıların elde edilmesi sağlanabilecek, yöneticilerin iş tatminleri ve motivasyonları artabilecektir. Burada sadece tepe yöneticilerin etkili bir lider olması yeterli olarak görülmemeli aksine liderlik yaklaşımları ile birlikte astların da kendilerini bir takım olarak hissetmeleri ve takım çalışmasının önemini anlayıp kavrayabilmeleri, güçlü örgüt ikliminin algılanması açısından son derece önemli olduğu kanısına varılabilir (Gayef, 2006).

2.2. BİLGİ YÖNETİMİNDE TEMEL KAVRAMLAR

2.2.1. Bilgi İle İlgili Temel Kavramlar

Bilgi, günümüzde üretim faktörü olarak değerlendirilebilmektedir. Kurumlar için vazgeçilemez, önemli bir değerdir. Kurumlar için en kritik varlık bilgidir. Kurumların değerleri, sahip oldukları bilgi ile ölçülmektedir. Bilgi, sadece bilgi teknolojileriyle işlenen bir varlık olarak düşünülmemelidir. Bilgi bir kurum bünyesinde çok değişik yapılarda bulunabilmektedir (e-dönüşüm, 2008).

Çağımız toplumlarının en temel hedefi, bilgi toplumu düzeyine erişebilmektir. Bilgi toplumlarında, stratejik kaynak olarak kabul edilen bilgi, bilgi teknolojilerinin sağladığı imkanlarla üretilmekte, sınıflandırılmakta, erişilebilir kılınmakta ve toplumsal, kurumsal sorunlarımızın çözülmesinde kullanılabilmektedir. Günümüzde bilgi, bireylerin, organizasyonların ve devletlerin sahip olabilecekleri en stratejik kaynak durumuna gelmiştir (Şimsek, 2002).

Bilginin yaşadığımız çağa damgasını vuran bir varlık olduğu bir gerçektir. Bu açıdan bakıldığında, çağımızın altın değerindeki hammaddesi olan bilgiyi tanımlamak, kavramak ve bilgi ile ilgili hususları incelemek, insanlığın başlangıcından itibaren geçen süreçte ileriye yönelik gelişimimizi şekillendirmenin en önemli anahtarıdır (Canber & Sağıroğlu, 2006).

İhtiyaç duyulduğu anda erişilemeyen bilginin hiçbir değeri yoktur. Bir başka ifade ile bilgi ulaşılabildiği oranda değerlidir ve ulaşılamayan bilgi sizin değildir.

2.2.1.1. Veri (data)

Veri, işlenmemiş ve yorumlanmamış gözlemler, islenmemiş gerçekler olarak da tanımlanabilir (Barutçiğil, 2002)**.**

Söz konusu muta; bir sayı, bir ifade, hatta bir resim olabilir ve ham haldedir. Verinin ham halde olması onun islenebileceği düşüncesini oluşturmaktadır (Cura, 2009).

Verilerin örgüt içinde kullanılabilmeleri için doğruluk, güncellik, güvenilirlik, eksiksizlik (tamlık), kullanılabilirlik, amaca uygunluk gibi birtakım özelliklere sahip olmaları gerekir (Saka, 2004).

Hastaneler ya da diğer sağlık kuruluşları verileri sağladığı kaynaklar; formlardan ve kayıtlardan bilgisayar ortamına aktarılan veri, veri tabanı yönetim sisteminden üretilen veri, sağlık araştırmalarından elde edilen veri, sağlık yönetim sisteminden elde edilen veri, telekomünikasyon, sağlık bilgi ağı ve kurumlar arası entegrasyondan üretilen bilgi, hastayla ilişkili veri (kodlama ve sınıflandırma sonucu üretilen veri, tıbbi görüntüleme sistemlerinden üretilen ve işleme ve analize tabi tutularak elde edilen veri, hasta kayıt sisteminden veri tabanına aktarılan veri) gibi farklı kaynaklardı (Saka, 2004).

2.2.1.2. Enformasyon

Bir gerçeği ifade eden ve ham halde bulunan veri, örgütsel ihtiyaçlar doğrultusunda belli bir amaca yönelik düzenlendiğinde anlamlı hale gelir ve kullanıcısına bazı mesajları iletebilir. Bu anlamlı mesajları taşıyan değerlendirilmiş verilere enformasyon (information) adı verilir. Enformasyon, düzenlenmiş veri olarak tanımlanabilir. Düzenleme başkaları tarafından yapılmıştır, yalnızca ilgili kişi için bir anlam taşımaktadır. Veriden çok daha zengin bir içeriği sahip olan enformasyon; yazılı, sözlü veya görsel bir mesajdır (Barutçiğil, 2002).

Peter Drucker'a göre ise enformasyon "ilişkiler ve amaç ile donatılmış veriler"dir (Davenport D, Prusak L.2001). Enformasyon; organize edilmiş, yapısal hale getirilmiş ve özetlenmiş veridir (Celep & Çetin, 2003).

Davranış değişiklikleri ve karar vermeyi sağlayacak şekilde insan aklı ile işlenip değerlendirme ve yorum katılmadığı sadece veriler hiçbir işe yaramamaktadır. İnsan faktörünün sadece dahil olması bilginin ortaya çıkarılması için vazgeçilmez bir unsurdur. Veri; girdi olarak kabul edilecek olursa, veri işleme sürecinin çıktısı enformasyon olacaktır (Cura, 2009).

Enformasyonun amacı alıcının bir konudaki düşüncelerini değiştirmek, değerlendirmesi ya da davranışı üzerinde bir etki yaratmaktır. Enformasyon, alıcısını biçimlendirmek zorundadır,

bakış açısında ya da anlayışında bir fark yaratmalıdır. Enformasyon, fark yaratan veridir (Davenport & Prusak, 2001).

Enformasyon kelimesi daha çok bilgiyi ve "diğerlerini" depolamakla, iletmekle ve çözümlemekle ilgilidir. Ayrıca enformasyon kavramı, bilimsel ve felsefi bilgi yanında, haberlerin, mesajların, fikir ve kanaatlerin iletimini de içermektedir (Yeniçeri & İnce, 2005). Enformasyon olayların doğası hakkındaki kavramları verirken, bilgi bu kavramları bir sebep-sonuç ilişkisi içinde tartışmaktadır (Dervişoğlu, 2004).

2.2.1.3. Bilgi

Buckland göre "bilgi" (information) terimini üç ayrı anlamda ele alarak tanımlamaktadır:

1) Süreç olarak bilgi (information-as-process);

2) Bilgi olarak bilgi (information-as-knowledge);

3) Nesne olarak bilgi (information-as-thing).

Yeni bir şeyler öğrendiğimiz zaman mevcut bilgilerimiz değişir ve yeni öğrendiklerimizle ilişkili olarak bazen mevcut bilgilerimizi gözden geçirmek durumunda kalabiliriz. İşte bu öğrenme eylemi, birisine bir şeyler aktarma ya da söyleme süreci "süreç olarak bilgi" olarak adlandırılmaktadır. Bu süreçte karşı tarafa aktarılan şeye ise "bilgi (knowledge) olarak bilgi" adı verilir. "Bilgi" terimi bilgilendirici, bilgi taşıyıcı nesneler (kitap, dergi, film, belge, vb.) için de kullanılmaktadır. Bu anlamda ise "nesne olarak bilgi"den söz etmek mümkündür. Bilgilenme sürecinde "süreç olarak bilgi" beynimizde meydana gelen değişiklikleri tam olarak açıklayamadığımız gibi, bu süreç sonunda edinilen bilgiyi (knowledge) elle tutup, gözle görmemiz ya da nesnel yöntemlerle ne kadar bilgi edindiğimizi ölçmemiz mümkün değildir. Bu süreç sonunda elde edilen bilgi (knowledge) ancak tanımlanarak nesneler üzerine aktarıldığı zaman (nesne olarak bilgi) elle tutulur, gözle görülür ya da ölçülebilir hale gelmektedir. Bilgi taşıyan nesneleri işleyerek yeni formlarda bilgi elde etmek ise "bilgi işleme" (information processing) olarak adlandırılmaktadır (Tonta, 2004).

İşlem kayıtları olan verilerin yorumlanması ile ulaşılan enformasyondan bir sonra gelinen aşama "bilgi"dir. Ham verilerin kullanılacak alana göre düzenlenmesi, sınıflandırılması, hatalardan arındırılarak belli mesajlar verebilecek şekilde enformasyon haline getirilmesinin ardından bu enformasyon, örgüt faaliyetinin niteliğine ya da ihtiyacına göre ilgili kişilerin zihinsel katkısı, faaliyette bulunulan sektördeki uygulamaların analizi ya da daha önce yararlanılarak başarıya ulaşılmış belli uygulamalar doğrultusunda yeniden bir değerlendirme sürecinden geçirildiğinde bilgiye ulaşılmış olunur. Elde edilen bilginin farklılık yaratması, süregelen uygulamaları olumlu yönde değiştirmesi beklenir. Bilgi; enformasyonun yorum, analiz ve bağlam ile zenginleştirilmiş halidir. Enformasyon olayların doğası hakkındaki kavramları verirken, bilgi bu kavramları bir sebep-sonuç ilişkisi içinde tartışmaktadır (Dervişoğlu, 2004).

Bilgiyi, üzerinde kesin bir yargıya varılmış, anlam kazanmış, kullanıcılar üzerinde davranış değişikliğine yol açabilen her türlü ses, görüntü ve yazılar olarak da ifade etmek mümkündür (Taşkın vd, 2001).

Bilgi, belli bir düzen içindeki deneyimlerin, değerlerin, amaca yönelik enformasyonun ve uzmanlık görüşünün, bir araya getirilip değerlendirilmesi için bir çerçeve oluşturan esnek bir bileşimdir (Davenport & Prusak, 2001).

Bilgi, enformasyonun belirli bir amaç için bağlantılı olarak kullanılmasıyla ortaya çıkar (Yeniçeri & İnce, 2005).

Bilgiyi çeşitli kriterleri baz alarak; düzenlenme ve kullanma tarzına göre, idealist, sistematik, pragmatik ve otomatik bilgi; kaynağına göre, örtülü ve açık bilgi; niteliğine göre, insanda, müşteride ve yapıda bulunan bilgi olarak sınıflandırabiliriz (Barutçugil, 2002). Bu sınıflandırmada anılan örtülü bilgi, açığa çıkarıldığında işletmeler için artı değer yaratması bakımından özellikle önemli görülmektedir. Açık bilgi ise gerek dokümanlar gerekse formel ve sistematik olarak aktarımı mümkün olan ve kodlanmış bilgi anlamına gelmektedir (Celep & Çetin, 2003).

D.Bell'e göre bilgi toplumunun gereklerini karşılayacak şekilde yaptığı tanımında bilgiyi "telif hakkı ya da başka bir sosyal tanıma yoluyla onaylanmış, bir isme veya isim grubuna bağlı, nesnel olarak bilinen entelektüel bir mülkiyettir" olarak tanımlamaktadır (Yeniçeri & İnce, 2005).

Bilgi, yeni deneyimleri ve enformasyonu değerlendirmek, içselleştirmek için bir ortam ve çerçeve sağlayan, deneyim, değerler, sözel enformasyon, uzman kavrayışı ve mesnetli sezginin esnek bir karışımıdır (Tiwana, 2003).

Haris'e göre bilgi "enformasyon, bağlam ve deneyimin bileşimi" olarak tanımlar. Bağlam bir kişinin hayata bakış açısını çizen çerçeve ise, sosyal değerler din, kalıtım, cinsiyet gibi unsurlarda bakış açısının ayrılmaz parçaları olarak karşımıza çıkar. Bu noktada önemli olan unsurlardan bir tanesi de iletim ile ilgilidir. Eğer bilgi bir kişiden başka bir kişiye iletiliyorsa artık bu bilgi alıcının bağlam ve tecrübesi ile algılanacak demektir (Dervişoğlu, 2004). Bilgi, daha özel bir durumda: "değer kazanmış enformasyon" olarak tanımlanabilir. Bu bağlamda bilgi ile enformasyon arasındaki içerik farkına değinmek yararlı olacaktır. Bilgi, enformasyonun belirli bir amaç için bağlantılı olarak kullanılması ile ortaya çıkar. Bilgi, enformasyonun yorum, analiz ve bağlam ile zenginleştirilmiş halidir (Yeniçeri & İnce, 2005).

Herhangi bir bilginin değer taşıyabilmesi için aşağıdaki özelliklere sahip olması gerekir.

- ***Doğruluk:*** Durumun adil bir şekilde ortaya konulabilmesi için bilgiler doğru olmalıdır. Her zaman yüzde yüz doğru bilgiye ulaşabilmenin mümkün olmadığı unutulmamalıdır.
- ***İlgililik***: Bilgi konuyla ilgili olmalıdır; aksi halde gereksiz işlemlere ve zamana mal olmaktadır.
- ***Tamlık:*** Bilgi tam olmalıdır; eksik bilgi sonuçların yanıltıcı hatta yanlış olmasına neden olabilmektedir. Gerçekte konuyla ilgili tüm bilgilerin toplanabilmesi imkânsız olduğu için en azından kritik bilgiler sağlanmalıdır.
- ***Doğru Zamanlılık:*** Bilgiye ihtiyaç duyulduğu anda hazır olmalıdır. Zamanında elde edilmeyen bilgi değerini yitirip boşa çaba haline gelebilmektedir.
- ***Ulaşabilirlik:*** Bilgiyi istenilen her anda kolaylıkla ulaşılmalıdır.
- ***Anlaşırlılık:*** Bilgi, kullanıcıyı terettüde sürüklemeden kolaylıkla anlaşılabilir olmalıdır.
- ***Güvenilirlilik:*** Kullanıcı bilgiye güvenmeli, gönül rahatlıyla kullanılabilmelidir.

- ***Etkin Maliyet***: Bilgini maliyeti bilgiden elde edilecek faydadan daha fazla olmalıdır. Bilginin toplam maliyeti rant oranını aşıyorsa, bilginin herhangi bir değeri kalmamaktadır (Yozgat, 1998).

Bilgi yalın ya da basit olamaz. Çeşitli unsurların birbirleriyle karışmasından oluşur, belli bir biçime sahip olmakla birlikte esnektir, sezgiler işin içerisine girdiğinde ona sözcüklerle sahip olmak ya da mantık terimleri kullanarak onu tümüyle anlamak zordur. Bilgi, bireylerin deneyimleri ile gelişir bilinir. Esasen bilgi kendisini değerli kılan özellikler yanında yönetilmesi zor bir süreci de anlatmaktadır (Davenport & Prusak, 2001).Veri ve enformasyonun tersine bilgi, değerlendirmeyi de içerir.

Bir hastanenin her gün hizmet verdiği hasta sayısı bir veridir. Bu veri ilgililere bir fikir vermez. Ancak güde 1000 hastaya hizmet verildiği gerçeği bir veridir. İncelenen kavrama ilişkin bir gerçeği göstermekle birlikte, herhangi bir yorum ya da karşılaştırma yapılamadığından anlamlı bir ifade değildir. Söz konusu "1000 hasta" verisi, hastaların aldığı hizmetler, yas grupları, ödeme şekilleri gibi niteliklerine göre sınıflandırıldığında, sıralandığında ve/veya örgütün ihtiyacına özgü bir sınıflandırmaya tabi tutulduğunda artık enformasyonun varlığından söz edilebilir. Enformasyon; bir fikir veya bir mesaj verir. Ancak karar vermek ya da bir yorum yapmak için enformasyon, bu haliyle hala yetersizdir. Hasta sayısının dağılımı, niteliği ve diğer değerlendirme alanları ile ilgili bilgi elde edebilmek için örgütün ve çalışanların birikimlerine, deneyimlerine ve algılarına ihtiyaç duyulur. Deneyim ve yorumun varlığı, enformasyonu bilgiye dönüştürür. Bilgiye ulaşma ve bilgiyi verimli kullanma konusunun temel amacı, kişilerin davranışlarında ve kararlarında bir değişiklik yaratabilmektir. Bilgi yönetimi temel olarak veri, enformasyon ve bilgi kavramlarının etrafında şekillenir (0nat, 2010).

2.2.2. Bilgi Güvenliği İle İlgili Temel Kavramlar

Pfleeger, bilgi güvenliğini bilgiye sürekli erişimin sağlanması, bilginin göndericiden alıcısına kadar gizlilik içerisinde, bozulmadan, değişikliğe uğramadan ve başkaları tarafından ele geçirilmeden bütünlük içerisinde güvenli bir şekilde iletimi olarak tanımlar (Tekerek, 2008).

Bilgi güvenliği, elektronik ortamlarda verilerin veya bilgilerin saklanması ve taşınması esnasında bilgilerin bütünlüğü bozulmadan, izinsiz erişimlerden korunması için, güvenli bir bilgi işleme platformu oluşturma çabalarının tümüdür (Canber & Sağıroğlu, 2006).

Bilgi güvenliği**;** bilginin gizliliğinin, güvenilirliğinin ve elverişliliğinin korunmasıdır (TS ISO /IEC 27001:2006).

Bilgi güvenliği, "bilginin bir varlık olarak hasarlardan korunması, doğru teknolojinin, doğru amaçla ve doğru şekilde kullanılarak bilginin her türlü ortamda, istenmeyen kişiler tarafından elde edilmesini önleme olarak" tanımlanır (Canber & Sağıroğlu, 2006).

Bilgi güvenliği bilgilerin izinsiz erişim, kullanım, ifşa edilmesinden, yok edilmesinden, değiştirilmesinden veya hasar verilmesinden koruma işlemidir. Bilgi güvenliği kavramı verilerin mahremiyeti, bütünlüğü ve ulaşılabilirliği ile ilgilidir (Ulaşanoğlu & Yılmaz & Tekin, 2010).

Bilgi güvenliği, kurumların bilgi envanterindeki varlıkların gizliliğini, bütünlüğünü, erişilebilirliğini tehdit eden risklerin tanımlanıp, bu konuda risk yönetimi gereklerinin yapılmasıdır. Risk yönetimi kapsamında bilgilerin maruz kalabileceği tehditler bilgilerin önemine, tehlikenin olabilirliğine ve gerçekleştiğinde etkisine göre şu seçeneklerden biri tercih edilir.

- Riskin azaltılması,
- Riskin kabul edilmesi,
- Tamamen üçüncü bir tarafa devredilmesi (sigorta etmek gibi) veya
- Risk kaynağının yok edilmesi seçeneklerinden biri tercih edilir.

Risklerin tanımlanması ISO 13335-1 standardında da gösterilmektedir. Bu standardın tanımı itibariyle bilgi güvenliği, bilginin risk yönetimini yapmaktır (ISO/IEC 13335-1).

Bilgi güvenliğine olan ihtiyacın neden ortaya çıktığını anlamak için zamanında ve doğru bilgi almanın önemini anlamak gereklidir. Bilgi güvenliğinin temel amacı doğru kişinin kısa zamanda doğruluğundan emin olunan bilgiye ulaşımını garanti altına almaktır. Bu ihtiyacı basitçe göz önüne sermek için Albay John R. BOYD"un OODA (Observe-Orient-Decide-Act = Gözle-Yönlendir-Karar Ver-Harekete Geç) döngüsü dediği gösterime bakmak gereklidir. Model, idari

olarak doğru verilmiş kararların kurumları, aradaki belirsizlikler, kargaşa, kaos, korku, şüphe, panik ve güvensizlik ortamından rekabetçi avantaja götürdüğünü anlatmaktadır. Bu kararları verebilmek için de doğru bilgiye, doğru zamanda, doğru kişilerin ulaşması gerekmektedir (Kovacich, 2003).

Şekil 1: Gözle-Yönlendir-Karar Ver-Harekete Geç Döngüsü (Kovacich, 2003).

Bilgi güvenliğinin sağlanmasında güvenlik politikaları ve standartlarının önemi büyüktür. Güvenlik politikaları üst yönetim tarafından desteklenen, kullanıcılar tarafından uygulanabilir ve anlaşılır olmalıdır. Kurum kültürüne uyan ve kurum genelinde kabul görmüş güvenlik politikaları olmaksızın bilgi güvenliğinin sağlanması ve yönetilmesi çok zordur.

Bilgi güvenliğinin sağlanabilmesi için teknik önlemlerin yanında, idari önlemler (kurallar, cezalar, yaptırımlar vb.), standartlar (ISO 27001, Ortak Kriterler vb.) ve insan faktörü göz önüne alınmalıdır. Tüm bu süreçler ele alındığında bilgi güvenliği karmaşık çözümler içeren ve yönetilmesi zorunlu olan yasayan bir süreç halini almıştır (Tekerek, 2008).

2.2.3. Bilgi Güvenliği Bileşenleri

Bilgi güvenliğinin sağlanabilmesi için, bilgi sistemleri gizlilik, bütünlük, erişilebilirlik gibi temel güvenlik bileşenlerinin gereklerini sağlamak zorundadır (Tekerek, 2008; Kumaş, 2007; Canber & Sağıroğlu, 2006; Doğantimur, 2009) .Bu üç temel bileşene, kayıt tutma, kimlik tespiti, güvenirlik ve inkâr edememe alt bileşenleri de eklenebilir: (Tekerek, 2008; Canber & Sağıroğlu, 2006).

1. Gizlilik (Confidentiality)

"Yetkisiz kişilere, süreçlere ve benzeri vb. açıklanmaması ya da teslim edilmemesi gerekli veri ya da programların özelliği.."(Kumaş, 2007).

"Bilginin sadece erişim hakkı olan yetkili kişilerce erişilebilir olduğunu garanti etmek" (TSE-17789:2002).

Gizli bilginin yetkisi ve izni olmayan kişilerin eline geçmesinin engellenmesidir (Doğantimur, 2009; Dinçkan & Öner, 2007).Gizlilik, statik ortamlar (disk, teyp, cd, dvd vb.) veya ağ üzerinde bir göndericiden bir alıcıya gönderilen dinamik ortamdaki veriler için sağlanmak zorundadır. Gizlilik ilkesinin sağlanmasında şifreleme algoritmaları kullanılır (Tekerek, 2008).

2. Bozulmamışlık (Bütünlük)

"Programların sistemin ve verilerin kötü niyetli olsun olmasın değiştirilmesi ve bozulmasına karşı korunması ya da korunmuş olmasıdır (Kumaş, 2007).

"Bilginin ve işleme yöntemlerinin doğruluğunu ve bütünlüğünü temin etmek" (TSE - 17789:2002).

Bilginin doğruluğunun ve tamlılığının sağlanmasıdır. Bilginin içeriğinin değiştirilmemiş ve hiçbir bölümünün silinmemiş ya da yok edilmemiş olmasıdır (Doğantimur, 2009).

"Bilginin bozuk, çarpık ve eksik olmamasıdır"(Aydınlı, 2009).

Bilginin göndericiden çıktığı haliyle bir bütün olarak alıcısına ulaştırılmasıyla bütünlük ilkesi sağlanır. Bilgi, haberleşme sırasında izlediği yollarda değiştirilmemiş, araya yeni veriler eklenmemiş, belli bir kısmı ya da tamamı tekrar edilmemiş ve sırası değiştirilmemiş şekilde alıcısına ulaştırılır. Verinin bütünlüğünün sağlanılması için özetleme algoritmaları kullanılmaktadır (Tekerek, 2008).

3. Kullanılırlık (Erişilebilirlik)

"Bir sistem yada özkaynağın gereksinildiğinde kullanıma elverişli olma derecesi…" (Kumaş, 2007; Dinçkan & Öner, 2007).

"Yetkili kullanıcıların ihtiyaç duyulduğunda bilgi ve ilişkili kaynaklara erişebileceklerini garanti etmek" (TSE -17789:2002).

Bilgi veya bilgi sistemlerinin kesintisiz şekilde kullanıma hazır veya çalışır durumda kalmasını hedefler (Aydınlı, 2009).

Bilgiye zamanında erişim, bilgi sistemlerini kullanan kişiler tarafından büyük bir önem taşımaktadır. Erişilebilirlik hizmeti, bilişim sistemlerini, kurum içinden ve dışından gelebilecek erişilebilirliği düşürücü tehditlere (Denial of Service Attack- DOS, DDOS) karşı korumayı hedefler. Bu bileşen sayesinde, kullanıcılar erişim yetkileri dâhilinde olan verilere güncel, zamanında ve hızlı bir şekilde ulaşabilirler. Sistem erişilebilirliği, bilgisayar yazılımlarındaki hatalar, sistemin yanlış, bilinçsiz ve eğitimsiz personel tarafından kullanılması veya konfigüre edilmesi, doğal felaketler gibi faktörler de sistem sürekliliğini etkileyebilir. Sisteme erişilebilirliğin sürekli sağlanması için fiziksel önlemler alınmalı, güvenlik duvarları, atak tespit sistemleri, antivirüs yazılımları kurulmalıdır (Tekerek, 2008; Doğantimur, 2009).

Bu üç temel unsur birbirinden bağımsız olarak düşünülememektedir. Bilginin gizliliğinin sağlanması o bilginin erişilebilirliğini engellememelidir. Aynı zamanda erişilebilen bilginin bütünlüğünün de sağlanması önemlidir. Eğer bir bilgi için sadece gizlilik sağlanılıyor ve bilgiye erişim engelleniyor ise kullanılamaz durumda olan bu bilgi bir değer ifade etmeyecektir. Eğer erişimi sağlanıyor ancak bütünlüğü sağlanmıyor ise kurumlar ve kişiler için yanlış veya eksik bilgi söz konusu olacak ve olumsuz sonuçlara neden olabilecektir. Dolayısıyla bilgi güvenliği kavramı temel olarak bu üç unsurun bir arada sağlanması demektir (Doğantimur, 2009).

4. Sorumluluk

Belirli bir eylemin yapılmasından, kimin veya neyin sorumlu olduğunu belirleme yeteneğidir. Tipik olarak etkinliklerin kayıtlarını tutmak için bir kayıt tutma (logging) sistemine

ve bu kayıtları araştıracak bir hesap inceleme (auditing) sistemine ihtiyaç duyar (Canber & Sağıroğlu, 2006).

Elektronik ortamda gerçekleşen olayları, daha sonra analiz edilmek üzere kayıt altına almaktır. Olay, bilgisayar sistemi ya da bilgisayar ağı üzerinde meydana gelen herhangi bir faaliyet olarak tanımlanabilir. Kullanıcının parolasını yazarak sisteme girmesi, web sayfasına bağlanması, e-posta iletişimi gibi örnekler verilebilir. Kayıt tutma saldırganların belirlenmesi içinde ayrıca bir önem arz etmektedir. Saldırı olduktan sonra kayıtlar yardımıyla iz sürülerek saldırganın kimliğinin tespit edilmesi sağlanır (Tekerek, 2008).

5. Güvenirlik (Reliability)

Bilgisayar sistemlerinden beklenen davranış ile elde edilen sonuçlar arasındaki tutarlılık durumudur. Başka bir deyiş ile güvenirlik, sistemden ne yapmasını bekliyorsak, sistemin kendisinden beklenileni yapmasını ve her çalıştırıldığında da aynı şekilde davranması olarak tanımlanabilir (Tekerek, 2008).

Bir bilgisayarın, bir bilginin veya iletişim sisteminin şartnamesine, tasarım gereksinimlerine sürekli ve kesin bir şekilde uyarak çalışması ve bunu çok güvenli bir şekilde yapabilme yeteneğidir (Canber & Sağıroğlu, 2006).

6. İnkâr Edememe (Non-Repudiation)

Bir bilgiyi alan veya gönderen tarafların, o bilgiyi aldığını veya gönderdiğini inkâr edememesini sağlama işlemidir (Canber & Sağıroğlu, 2006).

Bu bileşenle, ne gönderici alıcıya bir mesajı gönderdiğini, ne de alıcı göndericiden bir mesajı aldığını inkâr edebilir. Bu hizmet, özellikle gerçek zamanlı işlem gerektiren bankacılık ve finans bilgi sistemlerinde kullanım alanı bulmaktadır. Gönderici ile alıcı arasında ortaya çıkabilecek anlaşmazlıkların en aza indirilmesini sağlamaya yardımcı olmaktadır. Sayısal imza teknikleriyle inkâr edememe ilkesi sağlanır (Tekerek, 2008).

2.2.4. Bilgi Yönetimi

Adını bilgiden alan çağımız, bilginin yarattığı değerin tüm kurum ve bireylerce algılanmasından sonra, yöneticiler için bilgiyi elde etmek kadar yönetmekte bir o kadar önemli hale gelmiştir. Teknolojik gelişmeler bilgiyi transfer etme, depolama, saklama, sınıflandırma ve ihtiyaç duyulduğunda kullanıma sunma bakımından büyük kolaylıklar sağlamıştır. Bu yapının işlerlik kazanması ve işletmeler için değer yaratması ise yöneticilerin bilgi yönetimi konusunda ne kadar başarılı oldukları ile ilgilidir. O halde bilgi yönetimi ve işletmeler için önemi nedir sorusunu doğru cevaplamak için, bilgi yönetiminin ne anlama geldiğini ortaya koymakta fayda vardır.

"Bilgi yönetimi" kavramı, İngilizce'de "knowledge management" ve "information management" olarak karşılık bulmaktadır. Türkçe'de ise "information management" ile "knowledge management" arasındaki ayrım şu şekilde yapılabilir: "Information management" kayıtlı olan bilginin yönetilmesini ifade ederken "knowledge management", bir kurumun misyonunu yerine getirebilmesi için kurum çalışanlarının geliştirdiği ya da biriktirdiği deneyim, hizmet ve ürünlerden sağlanan bilgiden oluşan entelektüel sermayenin kullanımına dayanan bir yönetim uygulamasıdır (Tonta, 2004).

“Bilgi yönetimi” (information management; IM) her türlü örgütün etkin olarak işletilmesiyle ilgili bilginin sağlanması, düzenlenmesi, denetimi, yayımı ve kullanımına yönetim ilkelerinin uygulanmasıdır. Bilgi terimi burada örgüt içinde ya da dışında yaratılmış değerli bilgileri (üretim verileri, personel kayıtları ya da dosyaları, pazar araştırması verileri, çeşitli kaynaklardan toplanan rekabetçi bilgi) kapsamaktadır. Bilgi yönetimi örgütsel performans bağlamında bu bilginin değeri, kalitesi, sahipliği, kullanımı ve güvenliğiyle ilgilidir (Wilson, 2002).

Townley, bilgi yönetimini bir örgütün misyonunu gerçekleştirmek ya da amacına ulaşmak için aldığı kararları en etkili biçimde kullanmak suretiyle üretme ve paylaşma açısından bilgiyi kontrol altına alma faaliyeti şeklinde tanımlamaktadır (Yeniçeri & İnce, 2005).

Bilgi yönetimi en açık ifade ile bilgiyi yaratmak, elde tutmak, paylaşmak ve geliştirmek için kullanılacak yeni radikal yollar olarak tanımlanabilir (0nat, 2010).

Kirk Klasson'a göre "bilgi yönetimi, çekirdek iş yeteneğinden değer yaratmak ve daha çok değeri elinde tutma ehliyeti" olarak görülmektedir. Bu kavramın sınırları, "iş değeri yaratmak ve bir rekabet avantajı doğuracak örgüt bilgisinin yönetilmesi"ne kadar genişletilebilir. Bilgi yönetimi, temel olarak örgüt ortamında sürekli artan bilgi kapasitesini güncellemek, işlenen bilgilerin ulaşılabilir ve gerekli olanlarını ve bunlara ulaşmak için gerekli işlemlerin tanımlanması ve analizini kapsayan ve bunların örgüt çalışanlarıyla paylaşılmasını sağlayan bir disiplindir (0nat, 2010).

Bilgi yönetimi; insanların yeterliliklerini, deneyimlerini, uzmanlıklarını, yeteneklerini, düşüncelerini, eğilimlerini, uygulamalarını ve hayallerini etkili olarak örgütler. Bilgi kaynaklarının parçaları olarak ifade edilen bu nitelikleri örgütsel ve kişisel uygulamalar ile örgüt içerisine katar ve örgütsel amaçlara ulaşılması için örgütle bütünleştirir. Todd, bu tanım ile bilgi yönetimini bütüncül bir yönetim uygulaması olarak algıladığını göstermiştir. Bu bütüncül yönetim uygulaması, örgütün sahip olduğu tüm enformasyon, bilgi ve bilgeliği örgütteki bireylerin kullanmalarını, birbirleri ile etkileşime girmelerini ve değerlendirilmelerini sağlamaktadır (0nat, 2010).

Bir diğer tanımda bilgi yönetimi; "örgüt süreçlerinin, enformasyon teknolojilerinin, veri ve enformasyon üretme kapasiteleri ile çalışanların yaratıcılık ve yenilikçilik kapasitelerinin sinerjik olarak kullanılmasına imkân sağlayacak biçimde yönetilmesidir" şeklinde ifade edilmektedir. Bu yaklaşımda bilgi yönetiminin iki ana unsuru olarak teknoloji ve insan gösterilmekte ve bu iki unsur arasında bir sinerji meydana getirmenin, örgüt hayatta kalabilmesi açısından stratejik öneme sahip olduğuna dikkat çekilmektedir (0nat, 2010).

Tıp ve sağlığa yönelik bilgi yönetimi şu şekilde tanımlanabilir: Bir tıp ya da sağlık kuruluşunun temelde hasta bakımına yönelik misyon ve amaçlarına ulaşmak ve performansını geliştirmek üzere, bütün enformasyon varlıklarını sistemli bir şekilde belirlemesi, elde etmesi, düzenlemesi, geliştirmesi, değerlendirmesi ve erişilebilir kılmasını, onların yayımı, paylaşılması, kullanılması veya uygulanmasını bütünleşik bir yaklaşımla sağlayan bir süreçtir (Alkan, 2003).

Bilgi yönetiminin ne olduğunu açıklandıktan sonra ne olmadığını da ortaya koymak yararlı olacaktır (O'Dell & Grayson & Essaıdes, 2003).

- Bilgi yönetimi bir din ya da manevi bir akım değildir.
- Durumlarından hoşnutsuz çalışanları ilginç bir felsefi bir kavram ile oyalama çabası değildir.
- Gerçeği bulma yolunda var oluşçu bir arayış değildir.
- Bir bilim ya da disiplin değildir.
- Son yılların yönetim modası değildir .

Çapara göre bilgi yönetiminin özellikleri:

• Bilgi yönetiminin konusunu kuruma ait örtük, açık, dış ve iç bilgi ile bu bilgiye ilişkin işlemler oluşturur. Temel çabası bilgiyi üretken kılmaktır. Entelektüel sermayenin kurum içerisinde en verimli biçimde kullanılmasını, yani bilimsel olarak yaratılan bilginin kurumsal alana transferini sağlar.

• Bilgi yönetimi uygulamalarında bilgi ve iletişim teknolojisi, iletişim, yeni ekonomi, bilgi bilimi, organizasyon, finans, psikoloji, sistem analizi, sosyoloji, linguistik, mühendislik alanlarından yararlanan disiplinler arası bir faaliyettir.

• Bilgi yönetimi sürekli bir uygulamadır. Bilgi Yönetimi her kuruluşun ve kuruluşta çalışan kişilerin özel gereksinmeleri doğrultusunda oluşturulur ve gözden geçirilir. Bu özelliği ile, genel problemleri çözmek üzere geliştirilmiş bir süreç, işlemler bütünü ve araç olan bilgi teknolojilerin farklılık gösterir.

• Örtük bilginin açığa çıkarılmasını sağlayarak kurum için önemli ve kritik olan bilginin kurum dışına çıkmasını önler (Çapar, 2003).

Yukarıda özellikleri ortaya konan bilgi yönetimini güçleştiren kimi unsurlar da (Barutçugil, 2002) şöyle sıralamaktadır:

• Bilgideki değişme hızının artması

• Teknolojik yapının, değişimi hızlandıracak şekilde karmaşıklaşması

• Organizasyonların teknolojik gelişme sonucunda daha karmaşık bir nitelik kazanması

• Çalışanların niteliklerinin ve eğitim düzeylerinin değişmesi

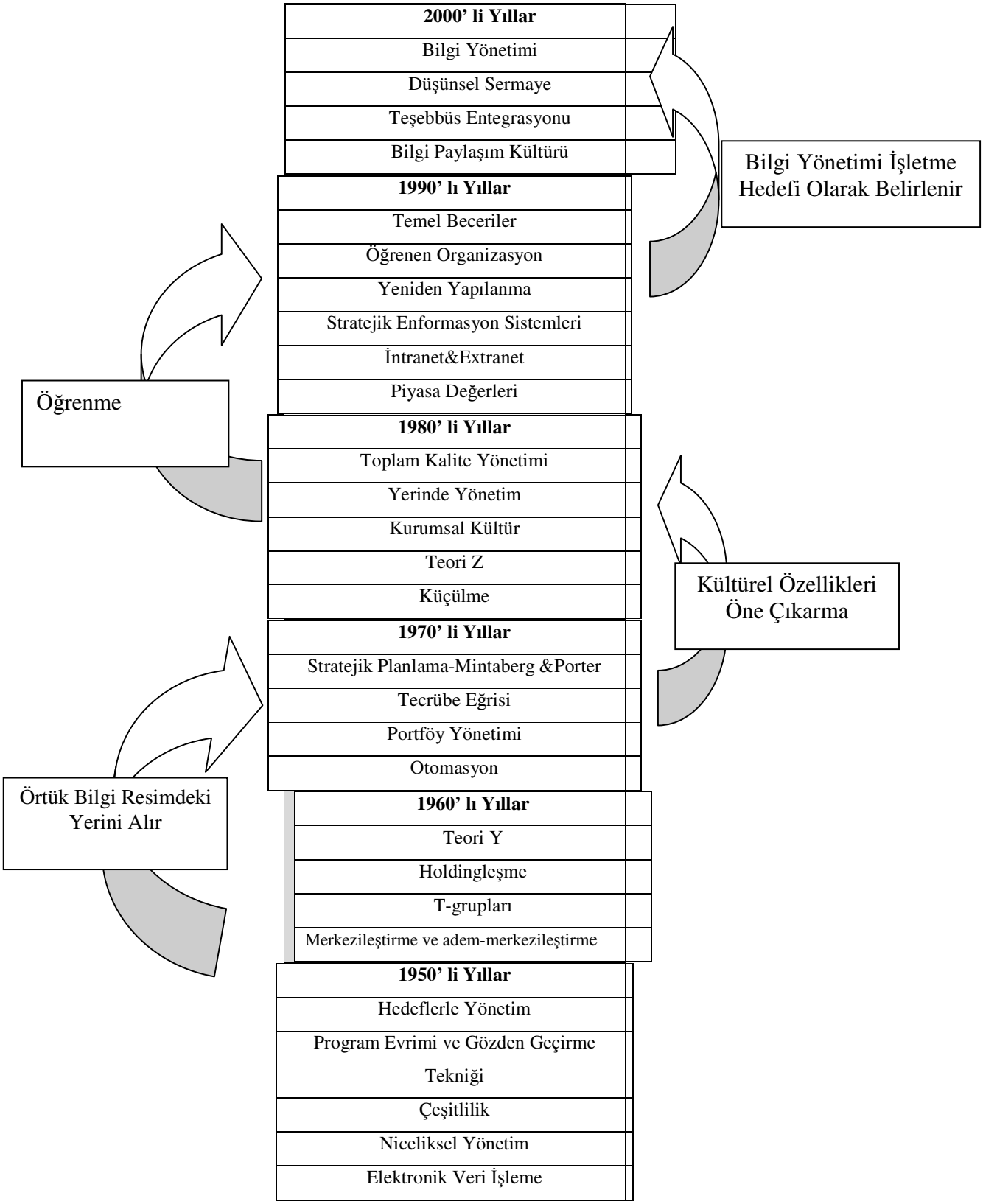
• Çalışanların beklentilerinin değişmesi

• Geleneksel hiyerarşik otoritenin yerini, yetenek ve bilginin alması.

Bilgi yönetimi hızlı teknolojik gelişmelerin ve yeniliklerin bir sonucu olarak kendinden söz ettirmiştir. Hızlı değişimlerin en çok görüldüğü alan günümüzde iletişim ve bilgi teknolojilerindeki gelişmelerdir. Bilgi yönetimi geçmişe de usta-çırak ilişkilerinin aktarıldığı uygulana gelen bir yönetim olmakla birlikte, üst düzey yönetimlerin bilgi yönetiminden söz etmesi, 1990'lı yılarda olmuştur. Sanayileşmiş ekonomilerin temelinin doğal kaynaklardan entelektüel varlıklara kaymasıyla birlikte, yöneticiler kendi işlerinin temelinde yatan bilgiyi ve bu bilginin kaynağını araştırmaya yönelmişlerdir. Diğer yandan da, şebekeye bağlı bilgisayarların ortaya çıkışı, belirli türden bilgileri, her zamankinden daha kolay ve ucuz bir şekilde kodlaştırmayı, saklamayı ve paylaşmayı mümkün hale getirmiştir (Karahan & Yılmaz, 2010).

Bu gelişmeler bir yandan bilgi yönetiminin gerekliliğini geliştirirken ve bu yönde örgütsel yapılanmalar gerçekleştirilirken, diğer yandan da en önemli özelliği bilginin açıklığı, kolay ve hızlı bir biçimde ulaşılabilirliği olan bilgi toplumu oluşumunu hızlandırmıştır.

Şekil 2'de 1950'lerden 2000'lere ulaşan dönemde, yöneticilerin başvurduğu gözde araçların evrimi gösterilmektedir. Bu süreç günümüzde bilgi yönetimi diye adlandırdığımız gelişme ile noktalanmıştır.



Şekil 2: Bilgi Yönetiminin 1950'lerden Günümüze Gelişimi (Tiwana, 2003).

2.2.4.1. Bilgi Yönetiminin Amacı

Bilgi yönetiminin amacı, her türlü bilginin ona gereksinimi olana, gerektiği zamanda uygun biçimde sunulmasıdır. Bilginin dağıtımında onun hangi bağlamda kullanılacağı önem kazanır. Her türlü bilginin sunulması, aşırı haber yüklemesine (information overload) yol açabilir. Haber bombardımanı altında işe yarar bilgi bulmakta zorluk çekilebilir. Öte yandan, her birime sadece o birimi ilgilendiren bilginin sunulması, ilgili birimin bazı bilgilere ulaşamaması ve böylece öğrenme ve bilgi üretme olanağının elinden alınması anlamına gelmektedir. Üstelik bilginin kontrolü ya da kısıtlanarak sunulması, çalışanların yönetime güvensizliğine ve işe güdülenememesine yol açabilir. Örgütün farklı birimlerine farklı bilgilerin sunulması, birimlerin genellikle durumun bütünüyle ilgili farklı görüntülerden hareket ederek etkinlik yürütmesine, böylece alt birim hedeflerinin neredeyse kendi başına amaç haline gelmesine yol açabilir (Dixon, 1994).

Bilgi Yönetimin amaçlarını ise Çapar şöyle sıralamaktadır (Çapar, 2003).

• Örgüt içerisinde yeni bilginin üretilmesi,

• Dış kaynaklardaki değerli bilginin örgüte kazandırılması,

• Örgütsel kararlarda ulaşılabilir bilginin kullanılması,

• Bilginin dokümanlar, veri tabanları ve yazılımlar aracılığı ile (yani mevcut örgütsel bilgi varlıkları ile) sunulması,

• Toplumsal kültür ve özendiricileri ile bilginin büyümesini kolaylaştırması (daha makro düzeyde),

• Örgütün birimleri içerisinde oluşan bilginin veya başka örgütlerdeki benzer birimlerin, birimler arası transferinin gerçekleştirilmesi,

•Örgütsel bilginin kıymetlendirilerek entelektüel sermayeye çevrilmesi ve bilgi yönetimi sayesinde ölçülmesi.

Odabaş'a göre ise bilgi yönetiminin en önemli amacı, "organizasyonlarda var olan kayıtlı ya da potansiyel bilgi kaynaklarını ortaya çıkarmak ve iş süreçlerine dahil etmektir. Bilgi

yönetiminin diğer bir amacı ise, çalışanların var olan enformasyona erişimini mümkün kılarak enformasyon kaynaklarından yeni bilgilerin üretilmesini sağlamaktır"(Odabaş, 2005).

Bu amaçlarla oluşturulan bilgi yönetiminin önemi ise Nonaka tarafından şu şekilde ifade edilmektedir: "Kesin olan tek şeyin belirsizlik olduğu bir ekonomide sürekli rekabet üstünlüğünün tek güvenilir kaynağı bilgidir. Piyasalar değiştiğinde, teknolojiler çoğaldığında, rakipler fazlalaştığında ve ürünler neredeyse bir gecede eskidiğinde başarılı firmalar, istikrarlı biçimde yeni bilgi üretebilen, bu bilgiyi organizasyonun her yerine geniş ölçüde yayabilen ve yeni teknolojilerde ve ürünlerde hızla kullanabilen firmalardır"(Nonaka, 1999).

Özgener ise bilgi yönetimin temel amaçlarını, öğrenme eğrisini hızlandırmak, daha hızlı iyileştirmeyi sağlamak, doğru bilginin doğru insanlara doğru zamanda ulaşmasını sağlamak, hızlandırılmış transformasyona imkan sağlamak, bilgi yönetiminin nihai amacı entelektüel sermayeden yararlanmak, özel olarak bilgi transferini teşvik etmek ve bilgi paylaşımını sağlamaktır, yetenekli bilgi çalışanı olan kurumlar tarafından başarılı bir toplum geliştirmek (Yeniçeri&İnce, 2005).

2.2.5. Bilgi Güvenliği Yönetim Sistemleri

Geçmişe bakıldığında bilgi sahibi kişilerin yüceltildiği, bilgi edinme amacıyla yapılan çabaların övüldüğü görülmektedir. Geçmişten günümüze kadar bilginin korunması nemli olmuş, bunu için büyük çabalar gösterilmiştir. Bugün ise, bilgi üretmek her örgütün hedeflediği fakat çok güç olan bir iş haline gelmiştir. Çünkü örgütün kapasitesi ve etkinliği üzerinde çok önemli etkileri olan bilgi, yenilikler için teknolojik üretimin de ön koşulu olup önemli avantajlar kazandıran bir unsurdur (Sawhney, 2001). Teknolojilerin gelişmesiyle iletişimin ve işbirliğinin son derece kolaylaştığı günümüz bilgi çağında, bilginin önemi ve gücünden dolayı, bilgi üretme ve bilgiyi yönetme ayrı bir sorun olarak karşımıza çıkmaktadır. İleri toplum biçiminin önem kazanan tarafları olduğu gibi, bilgi çağında ise, önem kazanan bilgi ve bilgi üretimi olmuştur. Çünkü çağdaş örgütlerde ihtiyaç duyulan bilgi miktarı gün geçtikçe arttığı gibi, günümüzün ekonomik, sosyal, politik örgütlerinin daha karmaşık yapıya bürünmeleri, bunların yönetimi ve denetiminde de daha fazla bilgiye ihtiyaç duyulmasına yol açmıştır (Taşkın vd., 2001).

İçinde bulunduğumuz enformasyon çağında bilgi bireysel, kurumsal, toplumsal ve küresel düzeyde stratejik bir kaynak olmuş, her alanda geleneksel yaklaşımların yerini, teknoloji ve

bilgiye dayalı yeni yaklaşımlar almıştır. Bilgi yönetimi, 1990'ların ortalarında enformasyon ve iletişim teknolojilerinin, bilgiye dayalı yeni ekonominin, iş dünyasındaki küresel rekabetin ürünü olarak ortaya çıkmıştır. Şirketler, tek başına teknoloji kullanımının, artan rekabet ortamında avantaj sağlayamadığını, daha çok enformasyonun kendisinin kullanımının, özellikle enformasyonun bilgiye dönüştürülmesinin verimliliği artıracağını ve bilginin temel rekabet silâhı olduğunu fark etmişlerdir. Bu durum, şirket bilgisinin yönetilmesi gerektiğini gündeme getirmiştir. İşte bilgi yönetimi, günümüzün karmaşık toplumsal, ekonomik, teknolojik koşullarının etkisiyle böyle ortaya çıkmıştır. Bilgi yönetimi yalnız iş dünyasında değil, kamu kesiminde, mal ve/veya hizmet üreten, kâr amacı güden, gütmeyen bütün kuruluşlarda, performansı geliştirmek üzere uygulanır olmuştur. Akademik tıp ve sağlık bilimleri kuruluşları, hastaneler, sağlıkla ilgili dernekler de, bilgi yönetiminin uygulandığı alanlar arasında yer almışlardır (Raymond, 2004).

Bilgi güvenliğinin sağlanması, güvenlik önlemlerinin seçilmesi ve uygulanması ile sınırlı değildir. Sürekli olarak yeni güvenlik açıkları ve saldırıların ortaya çıkması, kurum bilgi sistemlerinde teknolojik gelişmeler sonucu meydana gelen değişiklikler göz önüne alınarak güvenlik önlemlerinin düzenli olarak kontrol edilmesi, gerektiğinde iyileştirmeler ve değişiklikler yapılması gerekliliğini ortaya çıkarmaktadır.

Bilgi güvenliğinde sürekliliğin sağlanması için, tüm bu faaliyetlerin kurum ihtiyaçları ve kaynaklar göz önünde bulundurularak etkili ve verimli bir şekilde yönetilmesi gerekmektedir.

Etkili ve verimli yönetim ise Bilgi Güvenliği Yönetim Sistemi (BGYS) ile mümkün olup, bu amaçla tüm kurumlarda BGYS kurulması gerekmektedir (e-dönüşüm, 2009).

Bilgi Güvenliği Yönetim Sistemi (BGYS), kurumun hassas bilgilerini yönetebilmek amacıyla benimsenen sistematik bir yaklaşımdır. Bu sistemin temel amacı hassas bilginin korunmasıdır. Bu sistem çalışanları, iş süreçlerini ve bilgi teknolojileri (BT) sistemlerini kapsar (Dinçkan & Öner, 2007).

Her kurumun doğal faaliyetleri sonucunda belge ürettiği, bu belgelerin de işe yarar bilgileri ihtiva ettiği muhakkaktır. Kurumların kendi bilgilerinden maksimum derecede faydalanmaları ise etkin bir bilgi yönetimi sistemi ile mümkün olur. Etkin bir bilgi yönetimi süreci, kurumların bilgi

kullanım hızını artırır, maliyeti düşürür ve hem kurum çalışanlarına hem de müşterilerine ihtiyaç duyulan bilgi ve hizmeti sağlar (Audrey & Smith, 2001).

Kurum bünyesinde yaratılan, işlenen, depolanan, iletilen, imha edilen ve kullanılan bilgi ile kurumlar arasında iletilen bilginin gizliliği, bütünlüğü ve erişilebilirliğini korumak güvenliğin temel hedefidir. BGYS bu temel hedefi gerçekleştirmek amacıyla tasarlanmalıdır (e-dönüşüm, 2009).

Bilgi Güvenliği Yönetim Sistemleri (BGYS); insanları, süreçleri ve bilgi sistemlerini içine alan ve üst yönetim tarafından desteklenen bir yönetim sistemidir. Kurumlar açısından önemli bilgilerin ve bilgi sistemlerinin korunabilmesi, risklerin en aza indirilmesi ve sürekliliğinin sağlanması, BGYS'nin kurumlarda hayata geçirilmesiyle mümkün olmaktadır. BGYS'nin kurulmasıyla; olası risk ve tehditlerin tespit edilmesi, güvenlik politikalarının oluşturulması, denetimlerin ve uygulamaların kontrolü, uygun yöntemlerin geliştirilmesi, örgütsel yapılar kurulması ve yazılım/donanım fonksiyonlarının sağlanması gibi bir dizi denetimin birbirini tamamlayacak şekilde gerçekleştirilmesi anlamına gelmektedir. Kurumsal bilgi güvenlik politikalarının oluşturulması, BGYS kapsamının belirlenmesi, risk yönetimi, denetim kontrollerinin seçilmesi, uygulanabilirlik beyannameleri BGYS kurulabilmesi için, yapılması gereken adımlardır (Thow-Chang & Siew-Mun, and Foo, .2001; Aydınlı, 2009).

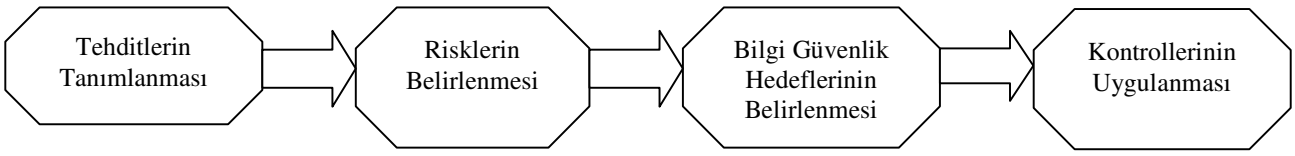
Bilgi güvenliği yönetim sistemi; Bilgi güvenliğini kurmak, gerçekleştirmek, işletmek, izlemek, gözden geçirmek, sürdürmek ve geliştirmek için, iş riski yaklaşımına dayalı tüm yönetim sistemlerinin bir parçası (TS ISO/IEC 27001:2006).

Bilgi güvenliğinin sağlanmasına yönelik olarak kurumlar tarafından maddi yatırımlar yapılmadığında meydana gelen zararların ekonomik boyutu her geçen gün katlanarak artmaktadır. Bilgi güvenliği ihlallerinin meydana getirdiği zararlar yapılması gereken güvenlik yatırımlarıyla kıyaslandığında farkın çok büyük olduğu güvenlik firmalarının yapmış olduğu araştırmalar tarafından açıkça görülmektedir.

Uluslararası denetim ve danışmanlık firması Ernst & Young, Türkiye'nin de içinde bulunduğu 50'yi aşkın ülke ve çeşitli sektörlerden yaklaşık 1400 kuruluşun katılımıyla "2008 Küresel Bilgi Güvenliği Anketi" adlı bir çalışma gerçekleştirip bilgi güvenliğinin önemini vurgulayan sonuçlarını yayımlamıştır. Ankette, bilgi güvenliğinin doğru uygulanmasının kurum

itibarını doğrudan etkilediği sonucu ortaya çıkmıştır. Katılımcıların yüzde 85'i bir bilgi güvenliği ihlali durumunda ortaya çıkan durumun, marka kimliği ve itibarına zarar verdiğini savunurken, yüzde 72'si gelir kaybına neden olduğuna değinmiştir. Söz konusu Türk katılımcılar, bilgi güvenliğinin kağıt üzerinde bir zorunluluktan ibaret olmadığını düşündüğü görülmüştür. Türkiye'deki Bilgi Güvenliği Yönetimi Sistemi'ni, ISO 27001 gibi sertifikasyon amacı gütmeden kurduğunu belirtenlerin oranı, ankete katılanların yarısını oluşturuyor (Doğantimur, 2009).

Bilgi Güvenlik Yönetim Sistemi dört aşamadan oluşmaktadır. Bu süreç şirket bilgi kaynaklarına saldırıda bulunabilecek tehditlerin belirlenmesi, tehditlerin yükleyebileceği risklerin belirlenmesi, bilgi güvenlik hedeflerinin oluşturulması ve risklere karşı kontrollerin uygulamasını kapsar. Tehditler mutlaka kontrol edilmesi gerekli riskleri ortaya çıkarır. Bu riskler şirketin bilgi kaynaklarına zarar vermeden ortadan kaldırılması yada azaltılmasına yönelik risk yönetimi uygulanmasını gerektirir. Bilgi Güvenlik Yönetim Sistemi kurulumuna yönelik süreçler Şekil: 3 'de sıralanmıştır (Raymond, 2004).



Şekil 3: Bilgi Güvenliği Yönetim Süreci (Raymaond, 2004).

Hansche göre bilgi güvenliği, bilgi teknolojileri çalışanlarının değil, üst yönetimin temel işidir ve kurumlarda güvenliğin gereklerinin yerine getirilip getirilmediğini bizzat üst yönetim sorgular. Güvenlik aşağıdan yukarı uygulanamaz, bilişim çalışanları kurum çalışanlarını güvenlik kurallarına uymaya zorlayamaz, bunu her kurumda üst yönetimin yapması gereklidir. (Yıldız, 2007)

İlk aşama, kurumun güvenlik önlemleri almak için örgütlenmesidir. Üst yönetimin başkanlık ettiği bir kurul, kurumun uzun vadeli stratejik bilgi teknolojileri ve güvenlik hedeflerini belirlemek ile işe başlar. Kurulda sadece bilgi teknolojileri çalışanları ya da bilgi teknolojilerine yakınlık duyan insanların olması hata olacaktır. Elden geldiğince çok birimden, değişik alışkanlık ve görüşten insanın olması, çalışmaları olumlu yönde etkileyecektir. Stratejik hedefler belirlendikten sonraki aşama taktik hedeflerin belirlenmesidir. Taktik hedefler ile kurumun

sunduğu ürün veya hizmetlerde nasıl bir değişikliğin kurumu stratejik hedeflerine ulaştıracağı ve bunların nasıl güvenlik ihtiyaçları doğuracağı belirlenir.

İkinci aşama ise operasyonel hedeflerin belirlenmesidir. Bu aşamada ise daha detaylı olarak günlük çalışmalarda yukarıdaki hedeflere nasıl ulaşılacağı kararlaştırılır.

Üçüncü aşamada kurum kültürü ve kurum yapısına göre ne gibi güvenlik önlemleri alınması gerektiği tartışılır. Örneğin bir özel şirketin öncelikli güvenlik hedefi yüksek erişilebilirlik iken, kamu kurumlarının hedefi gizliliktir. Bu hedefler belirlenirken kurum kültürünün ön planda tutulması çok önemlidir. Çünkü bu konuda ortaya çıkacak bir aksama veya çalışanların işlerini yapamamalarından dolayı güvenlik kurallarını toplu olarak hiçe saymaları, güvenlik çalışmalarına büyük darbe vuracaktır.

Dördüncü aşamada ise kurumun bilgi varlıklarını ve verileri sınıflaması gerekmektedir. Veriler gizlilik derecelerine, önemlerine, tarihlerine göre çıkarılıp sınıflanırlar.

Beşinci aşama riskleri belirlemektir. Riskleri belirlemeye fiziksel risklerden başlanmalıdır. Kurumun teyp yedekleme disklerinden, bilgisayarlara, sunuculara ve bağlantılarına kadar tüm varlıklarının bir listesi çıkarılıp bunların maruz kalabileceği tehlikeler ve tehditler belirlenir. Neyin nerede tutulması gerektiği, bakım ve garantilerin hepsi bu çalışmada göz önünde tutulmalıdır.

Altıncı aşama insanlardan kaynaklanabilecek riskler incelenmelidir. Burada kurumun iş yapma tarzları, çalışanların görev tanımları ve bu tanımlara göre erişim yetkilendirmelerinin belirlenmesi gerekir. Olası bilgi hırsızlıkları ve kuruma yapılabilecek sanal saldırılar bu aşamada değerlendirilir. Burada riskler belirlenirken bu risklere karşı alınacak önlemler de tartışılır. Burada önemli olan sadece alınacak önlemler değildir, bunların birbirlerine göre önem sırasına da karar verilmelidir.

Tüm bu çalışmalar yapılırken her aşamanın dokümante edilmesi önemlidir. Güvenlik çalışmalarının aynen kalite çalışmaları gibi bir sonuç üretmeye çalışmadığı, kalite çalışmaları gibi her asli sürecin altında çalışan bir alt fonksiyon olduğu akılda tutularak, her adım yazılır. Böylece ileride çalışmalar yeniden gözden geçirildiğinde hangi kararın neden verildiği ortaya konabilecektir .

Bilgi yönetim sisteminin sağlıklı işlemesi, yöneticilerin bilginin önemini algılama düzeylerine bağlı bir olgudur. Ancak yönetici, her bilgi yerine, hangi bilgiye sahip olması

gerektiği konusunda yetkin ve yeterli olmalıdır. Başka bir deyişle, işletme için fayda sağlamayacak bilgiye sahip olma tuzağına düşmemelidir (Demirel & Seçkin, 2008).

Nicolas'a göre bilgi yönetim stratejileri genel olarak üç grupta toplanmaktadır. Bunlar: teknolojik ağırlıklı stratejiler, birey ağırlıklı stratejiler ve sosyal süreçlere yönelik stratejilerdir (Özdemirci & Aydın, 2008). Bilgi yönetim uygulamalarının başarılı bir biçimde uygulanabilmesi için öncelikle kurumun iş strateji ile bilgi yönetim stratejisi arasında vazgeçilemez bir bağ olması gerekmektedir. Çoğu bilgi yönetimi projesinin öncelikli olarak odaklandığı nokta, yeni enformasyon teknolojisi araçlarının geliştirilmesidir. Etkin bir bilgi yönetim stratejisi, aslında sadece bir teknoloji stratejisinden ibaret değildir. Bu strateji; teknolojinin, kültürel değişimin, yeni bir ödüllendirme sisteminin ve şirketin iş stratejisine mükemmel biçimde uyum sağlamasına yönelik bir odaklanmanın dengeli bileşimidir. İyi uyarlandıkları ve bütünleştirildikleri takdirde, teknik ve kurumsal girişimler, bilgi yönetimi sürecini destekleyecek sağlam adımlar olurlar (Tiwana, 2003).

Günümüzde organizasyonlarda uygulanan birçok etkinlik teknolojiye dayandığı gibi, bilgi yönetimi uygulamasının da temelinde kolaylaştırıcı ve hızlandırıcı bir güç olarak teknoloji yer almaktadır. Özellikle bilgi teknolojileri organizasyonlara yeni fırsatlar sunmakta, verimli bir çalışma ortamı yaratmaktadır. Bilgi teknolojileri aynı zamanda rekabete yönelik önemli bir avantaj yaratmakta, bilgi yönetimi uygulamalarında önemli bir yer tutmaktadır (Yılmaz, 2008). Ulusların bilgi yönetimindeki başarısı bilgi teknolojilerine yaptıkları yatırım ve bilgi teknolojilerini kullanmadaki yaklaşımları ile sıkı ilişkilidir. O halde ulusların yaptıkları Ar-ge yatırımları ve genel bütçeden bilgi iletişim teknolojilerine ayırdıkları pay ile bilgi yönetimindeki başarı doğru orantılıdır.

Teknik aşamalar, verimli bir bilgi yönetimi sistemi kurulması açısından çözümü kolay olan kısımdır. Teknik olarak dünyanın en kusursuz bilgi yönetim sistemini dahi kursanız, bütün bu karmaşık sistemlerin en merkezinde "insan"ın yer alması, bu projeyi de "insan" merkezli bir proje haline getirmektedir. Bilgi üretmek ve bilgi paylaşmak, yani kurumsal içerik oluşturmak yaratıcı fonksiyonlardır ve bunlar insan merkezlidir. Bilgi güç ise, insanlar niçin bilgilerini ya da iyi projeler üretmelerini sağlayacak verileri başkalarıyla paylaşsınlar? Kurum ile çalışanları arasındaki bir bilgi yönetim sisteminin en karmaşık kısmı işte budur. İyi tasarlanmış bir bilgi yönetim sistemi, bilgisini paylaşan, işbirliği kuran çalışanların izlenip değerlendirilmesini

mümkün kılar. Paylaşmayı, işbirliği kurmayı ve değer üretmeyi ödüllendiren kültürel değişiklikler, bu sistemin hem gerekliliği hem de sonucudur. Bu sistemler aracılığıyla bilgi paylaşımını ya da beraber çalışma ortamını ölçmemiz mümkündür (Özdemirci &Aydın, 2008).

Bilgi güvenliği sadece bir Bilgi Teknolojisi (BT) ya da yaygın söylemle Bilgi Sistemleri işi değildir; kurumun her bir çalışanının katkısını ve katılımını gerektirir. Ciddi boyutta bir kurum kültürü değişimi gerektirdiği için, en başta yönetimin onayı, katılımı ve desteği şarttır. BT'nin teknik olarak gerekli olduğunu saptadığı ve uyguladığı teknik güvenlik çözümleri, iş süreçleri ve politikalarla desteklenmemiş ve kurum kültürüne yansıtılmamışsa etkisiz kalacaklardır. Gerekli inanç ve motivasyon yaratılamamışsa, çalışanlar şifrelerini korumakta özensiz, hassas alanlarda gördükleri yabancı kişilere karşı aldırmaz, kağıt çöpüne gerekli imha işlemini yapmadan atacakları bilgilerin değeri konusunda dikkatsiz olabilecekler ve yapılan güvenlik yatırımlarına karşın büyük bir açık oluşturmaya devam edebileceklerdir (Küçükoğlu, 2005).

Siponen'e göre çalışanların bilgi güvenliğinin önemine inanması ve bilgi güvenliği bilincine sahip olması, işletmelerde bilgi güvenliğinin sağlanmasında en önemli faktörlerdendir. Bilgi güvenliği ile ilgili tedbirlerin kullanılmaması, yanlış yorumlanması veya yanlış kullanılması güvenlik tedbirlerinin geçerliliğini kaybetmesine neden olmaktadır. Maslow'un ihtiyaçlar hiyerarşisinde güvenlik gereksinimi, fizyolojik gereksinimlerden sonra ikinci sırada anılsa da bilgi güvenliği söz konusu olduğunda bu sıralamaya uyulduğu söylenemez. İnsanlar, bilgi güvenliği ihlalleri sonucu genelde hayati zararlarla karşılaşmasalar da karşılaşabilecekleri kimlik hırsızlığı, kişisel bilgilerinin çalınması, işletme sırlarının çalınması, bilgilerinin silinmesi, değiştirilmesi ve yetkisiz olarak kullanılması vb. sorunları öngöremeyebilmektedirler (Acılar, 2009).

Bilgi güvenliğinin yönetiminin kurulmasında izlenmesi gereken adımlar (Vural & Sağıroğlu, 2008).

1-Bilgi güvenliği politikaları

2-BGYS kapsamı

3-Bilgi güvenliği standartları

2.2.5.1. Bilgi Güvenliği Politikaları

Bilgi güvenliği politikaları, bir kurumun değerli bilgilerinin yönetimini, korunmasını, dağıtımını ve önemli işlevlerinin korunmasını düzenleyen kurallar ve uygulamalar bütünüdür (Tuğlular, 2003).

Güvenlik politikaları kurum veya kuruluşlarda kabul edilebilir güvenlik seviyesinin tanımlanmasına yardım eden, tüm çalışanların ve ortak çalışma içerisinde bulunan diğer kurum ve kuruluşların uyması gereken kurallar bütünüdür (Vural & Sağıroğlu ,2008).

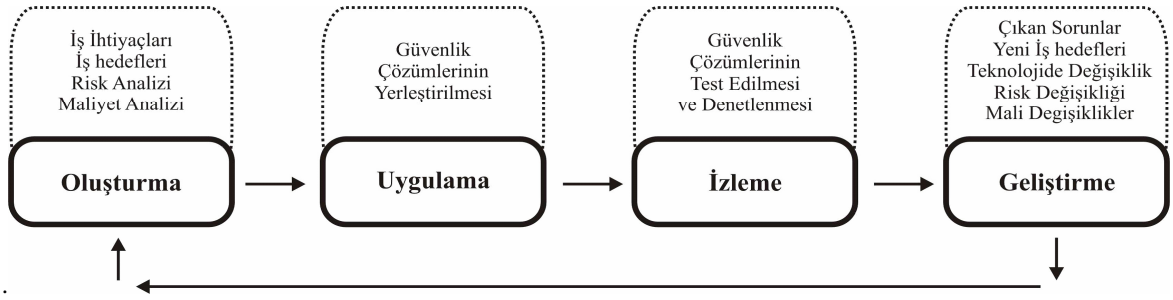
Hansche göre güvenlik politikası dokümanı uzun olmayan, temel güvenlik gereksinimlerini ve kurallarını açıklayan, kurallara uyulmaması halinde verilebilecek cezaları da içeren bir kurallar bütünüdür. Bu politika içinde kurumun bağlı olduğu kanuni ve ikili antlaşmalara dayalı kurallar da ortaya konmalıdır. Politikalar içerisinde tavsiye niteliğinde, kurum stratejisine uygun bulunan ya da karşı olan davranışlar da belirtilir. Bu politikalar kurumun en yüksek yöneticileri tarafından onaylanır. Politikalardan bir aşağı seviyede standartlar bulunur. Bunlar kurum içerisinde hangi işin, nasıl yapılması gerektiğine dair bir kural setidir. Standartlarda temel nokta uyumluluktur. Tüm kurumun aynı işleri aynı yollar ve araçlar ile yapmasını sağlamak için standartlar olmalıdır. Standartların kurum güvenlik politikası kadar kesin ve bağlayıcı olması gerekmemektedir. Daha aşağı seviyede ise rehberler gelmektedir. Rehberler özel bir işin nasıl yapılacağını açıklayan açıklayıcı eğitici dokümanlardır. Bu dokümanlar kurum çalışanlarının istedikleri zaman erişebilecekleri bir yerde depolanmalıdır. İşe alma ve işten çıkarma yöntemleri de güvenlik uygulamalarının bir parçasıdır. Kişi işten çıkarıldığı anda tüm erişim hakları da aynı anda engellenmelidir (Yıldız, 2007).

Güvenlik politikaları kurumun üst düzey yönetimi tarafından desteklenmeli ve çalışanlar tarafından benimsenmelidir. Güvenlik politikası uygulanabilir, kullanıcı tarafından anlaşılır, yapılabilir ve güvenlik yöneticileri tarafından kolay yönetilebilir olmalıdır. Bilgi güvenliği politikaları her organizasyon için farklılık gösterse de, tipik olarak çalışanın sorumluluklarını, kontrol mekanizmalarını, amaç ve hedefleri içeren genel ifadelerden oluşur (Vural & Sağıroğlu, 2008; Tekerek, 2008). Bu kural ve uygulamaları tanımlayan politikalar çeşitli seviyelerde yazılabilir. Politikalar, genel bir bilgi güvenliği politikası ve belirli alanlara ait politikalardan (erişim kontrol politikası, uzaktan erişim politikası, kullanıcı politikası, e-posta kullanım

politikası vb.) oluşur ve uygulamaları tanımlayan prosedür ve talimatlarla tamamlanır. Her seviyedeki politikanın tek bir dokümanda bulunması yerine, en üst seviyede temel ilkeleri barındıran bir Bilgi Güvenliği Politikası'nın oluşturulması ve bu dokümanla diğer ayrıntılı politikaların ilişkilendirilmesi tavsiye edilmektedir (Barman, 2001).

Bilgi güvenliği politikası, bu politikalar doğrultusunda uygulanacak prosedürlerin amaçlarını tanımlayan en üst düzey doküman olacaktır. Yeni bir ürünü tanımlayan teknik özellikler gibi, genel bir güvenlik programının planlarını oluşturacaktır.

Politikalar organizasyona özgü özel kanunlar olarak da düşünülmelidir. Her organizasyon içinde genel olarak Şekil: 4'de ifade edilen süreç işlemektedir Yöneticiler arasında yapılan bir araştırmaya göre, kurumlarında güvenlik teknolojisinin kullanılmakta olduğunu bildirenlerin oranı %70 olarak tespit edilmesine rağmen, yalnızca %38'nin yazılı bir güvenlik politikasına sahip oldukları belirlenmiştir (Tekerek, 2008).



Şekil 4: Bilgi Güvenliği Politikası Süreci (Tekerek, 2008).

Politikalar içerisinde; gerekçelerin ve risklerin tanımlandığı, kapsadığı bilgi varlıkları ve politikadan sorumlu olan çalışanların ve gruplarının belirlendiği, uygulanması ve yapılması gereken kuralların, ihlal edildiğinde uygulanacak cezai yaptırımların, teknik terimlerin tanımlarının ve düzeltme tarihçesinin yer aldığı yedi bölümden oluşur. Güvenlik Politikası içerisinde bulunması gereken bölümler Tablo 2'de özetlenmiştir. Belirli konularda çalışanın daha fazla bilgilendirilmesi, dikkat etmesi gereken hususlar, ilgili konunun detaylı bir şekilde ifade edilmesi istendiğinde alt politikalar geliştirilmelidir. Örneğin kullanıcı hesaplarının oluşturulması ve yönetilmesi şifre unutma, şifre değiştirme, yeni şifre tanımlama, e-posta gönderme ve alma konusunda, üst yönetimin kararlarını, kullanıcının uyması gereken kuralları ve diğer haklarını gibi durumlarda uyulacak kurallar alt politikalar aracılığıyla açıklanmalıdır. Alt politikayla üst

yönetimin, gerekli gördüğünde çalışanlarının e-postalarını okuyabileceği, e-postalar yoluyla gizlilik dereceli bilgilerin gönderilip alınamayacağı gibi hususlar, e-posta alt politikası içerisinde ifade edilebilir. Alt politikalar içerisinde, izin verilen yazılımlar, veritabanlarının nasıl korunacağı, bilgisayarlarda uygulanacak erişim denetim ölçütleri, güvenlikle ilgili kullanılan yazılım ve donanımların nasıl kullanılacağı gibi konular da açıklanabilir (Vural & Sağıroğlu, 2008).

Tablo 2: Güvenlik Politikası Kısımları (Vural & Sağıroğlu, 2008).

Bölüm Adı	İçeriği
Genel Açıklama	Politikayla ilgili gerekçeler ve buna bağlı risklerin tanımlamasını kapsar.
Amaç	Politikanın yazılmasındaki amaç ve neden böyle bir politikaya ihtiyaç duyulduğunu açıklar.
Kapsam	Politikaya uyması gereken çalışan grupları (ilgili bir grup veya kurumun tamamı) ve bilgi varlıklarını belirler.
Politika	Uygulanması ve uyulması gereken kuralları veya politikaları içerir.
Cezai Yaptırımlar	Politika ihlallerinde uygulanacak cezai yaptırımları açıklar.
Tanımlar	Teknik terimler ile açık olmayan ifadeler listelenerek açıklanır.
Düzeltme Tarihçesi	Politika içerisinde yapılan değişiklikler, tarihler ve sebepleri yer alır.

Kurumsal bilgi güvenliği politikaları kuruluşların ihtiyaçları doğrultusunda temel güvenlik unsurlarının (gizlilik, bütünlük, erişilebilirlik, vb.) bazıları üzerinde yoğunlaşabilir. Örneğin askeri kurumlarda, bilgi güvenliği politikalarında gizlilik ve bütünlük unsurları ön plana çıkmaktadır. Askeri bir savaş uçağının kalkış zaman bilgilerinin onaylanıp yürürlüğe girmesi için düşmanlar tarafından görülmemesi (gizlilik) ve değiştirilmemesi (bütünlük) gereklidir. Bir diğer örnek ise kâr amacı gütmeyen durumlarda uygulanan bilgi güvenliği politikalarında genellikle erişilebilirlik ve bütünlük unsurları ön planda gelmektedir. Üniversite sınav sonuçlarının açıklandığı yükseköğretim kurumunda uygulanan güvenlik politikasında öğrenciler sınav

açıklandıktan sonra istediği zaman diliminde (erişilebilirlik) doğru bir şekilde (bütünlük) sınav sonuçlarına bakabilmelidir.

İyi bir güvenlik politikası, kullanıcıların işini zorlaştırmamalı, kullanıcılar arasında tepkiye yol açmamalı, kullanıcılar tarafından uygulanabilir olmalıdır. Politika, kullanıcıların ve sistem yöneticilerinin eldeki imkânlarla uyabilecekleri ve uygulayabilecekleri yeterli düzeyde yaptırım gücüne sahip kurallardan oluşmalıdır. Alınan güvenlik önlemleri ve politikaları uygulayan yetkililer veya birimler yaptırımları uygulayabilecek idari ve teknik yetkilerle donatılmalıdır. Politika kapsamında herkesin sorumluluk ve yetkileri tanımlanarak kullanıcılar, sistem yöneticileri ve diğer kişilerin sisteme ilişkin sorumlulukları, yetkileri kuşku ve çelişkilere yer bırakmayacak biçimde açıkça tanımlanmalıdır. Politikalar içerisinde uygulanacak olan yasal ve ahlaki mahremiyet koşulları ile elektronik mesajların ve dosyaların içeriğine ulaşım, kullanıcı hareketlerinin kayıt edilmesi gibi denetim ve izlemeye yönelik işlemlerin hangi koşullarda yapılacağı ve bu işlemler yapılırken kullanıcının kişisel haklarının nasıl korunacağı açıklanmalıdır. Saldırıların ve diğer sorunların tespitinde kullanıcıların, yöneticilerin ve teknik personelin sorumluluk ve görevleri ile tespit edilen sorun ve saldırıların hangi kanallarla kimlere ne kadar zamanda rapor edileceği güvenlik politikalarında açıkça belirtilmelidir. Sistemlerin gün içi çalışma takvimleri, veri kaybı durumunda verinin geri getirilmesi koşulları gibi kullanıcının sisteme erişmesini sınırlayan durumlara politikalar içerisinde yer verilmelidir. Bu durumlarda kullanıcıya, izlemesi gereken yolu anlatacak ve yardımcı olacak kılavuzlara da yer verilmelidir (Vural & Sağıroğlu, 2008;Yıldız, 2007).

2.2.5.2. Bilgi Güvenliği Yönetim Sistemleri Kapsamı

BGYS'nin kapsamı kurumların sahip olduğu bilgi varlıkları ve ihtiyaçları doğrultusunda tespit edilir. Bu kapsam;

• Kurumun sahip olduğu bilgi varlıklarının tamamı,

• Bilgi sistemlerinin bir kısmı (Bilişim sistemleri, kâğıt ortamdaki bilgiler, elektronik bilgi varlıkları, vb.),

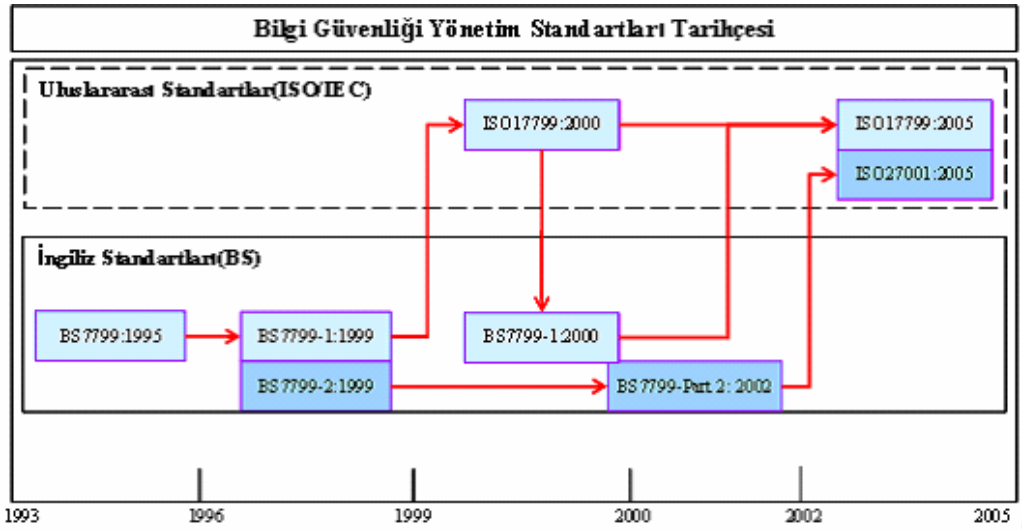
• Belli bir yerleşim birimindeki bilgi sistemleri (Merkez Binalar, Genel Müdürlükler, vb.),

• Odaklanılmış bir bilgi sistemi (bilgisayarlar, ağ sistemi, sunucu bilgisayarlar, web sunucusu, vb.) olabilir (Thow-Chang & Siew-Mun and Foo, 2001).

2.2.5.3. Bilgi Güvenliği Standartları

Tehditlerin sürekli olarak yenilenmesi, kullanılan yazılım veya donanımlarda meydana gelen güvenlik açıklarının takibi, insan faktörünün kontrolü gibi süreçlerin takip edilebilmesi ve üst seviyede bilgi güvenliğinin sağlanması, bilgi güvenliği sürecinin yönetilmesi için yapılan çalışmalar sonucunda İngiliz Standartlar Enstitüsü (British Standards Institute-BSI) tarafından 1995 yılında BS–7799 standardının ilk kısmı olan BS7799–1, 1999 yılında ise aynı standardın ikinci kısmı olan BS7799–2 İngiliz standardı olarak yayınlanmıştır (Vural & Sağıroğlu, 2008).

BS7799–1 2000 yılında küçük düzeltme ve adaptasyonlardan geçerek ISO tarafından ISO/IEC– 17799 adıyla kabul edilmiş ve dünya genelinde kabul edilen bir standart halini almıştır. 2002 yılında ise BSI tarafından BS–7799 standardının ikinci kısmı olan BS–7799–2 standardı üzerinde eklemeler ve düzeltmeler yapılarak ikinci defa İngiliz standardı olarak yayınlanmıştır. 2005 yılında ise ISO tarafından ISO/IEC–17799 standardı üzerinde eklemeler ve düzeltmeler yapılmış ISO/IEC–17799:2005 adıyla yeniden yayınlanmıştır. Son olarak 2005 yılında ISO İngiliz standardı olan BS7799–2 üzerinde eklemeler ve düzeltmeler yaparak ISO/IEC:27001 standardını yayınlamıştır. Bilgi güvenliği yönetim sistemlerinin temelini teşkil eden standartların yayınlanma süreleri Şekil: 5'de tarihsel akışa göre verilmiştir(Vural & Sağıroğlu, 2008).



Şekil 5: Bilgi Güvenliği Yönetim Standartları Tarihçesi (Vural & Sağıroğlu, 2008).

1.İngiliz Standartları (British Standart)

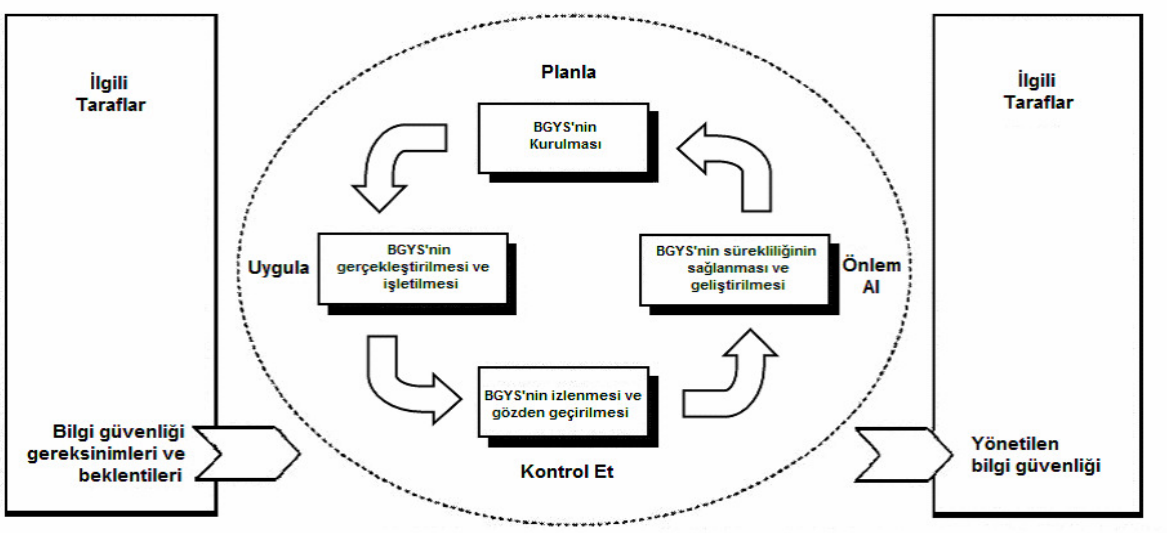
BS–7799, bilgi varlıklarının gizlilik, doğruluk ve erişilebilirliğini güvence altına almak için uygulanması gereken güvenlik denetimlerini düzenleyen ve belgelendiren iki aşamalı İngiliz standardıdır. 1999 yılında yayınlanan ilk sürümün birinci bölümünde bilişim güvenliği için çalışma kuralları anlatılmakta olup (Information Technology– Code of Practice for Information Security Management) 10 bölüm içerisinde 36 kontrol 127 alt kontrol maddesi bulundurmaktadır. İkinci bölümde (Information Security Management Systems– Specification with Guidance for Use) bilgi güvenliği yönetim sistemini planlamak, kurmak ve devam ettirmek için gerekli olan süreçler adım adım tanımlamakta ve bilgi güvenliği yönetim sistemine ait belgelendirme (sertifikasyon) bu kısımda yapılmaktadır.

BS–7799 kurumların sadece kendi bilgi güvenlik prosedürlerini değil birlikte çalıştıkları iş ortaklarıyla ilgili sözleşmelerinde bilgi güvenliği yönünden analiz edilmesine yardımcı olmaktadır. BS–7799 standardı endüstri, devlet ve ticari kuruluşlardan ortak bir güvenlik modeli oluşturulmasına gelen talepler sonucu BSI kuruluşu ve BOC, BT, Marks&Spencer, Midland Bank, Nationwide Building Society, Shell, Unilever ve diğer bazı şirketlerin katılımıyla hazırlanmış bir standarttır.

Standardın tarihsel oluşumuna bakıldığında 1993 yılında Kural rehberi, 1995 yılında İngiliz standardı, 1998 yılında Sertifikasyon tarifi yapılmış, 1999 yılında büyük bir düzeltmeden geçerek birinci kısmı, 2002 yılında ise ikinci kısmı yayınlanmıştır. BS–7799 standardı teknik ve idari bölümlerden oluşmaktadır. Standardın birinci kısmının ilk sürümünde yer alan etki alanlarının idari ve teknik kısımlara göre güvenlik politikası, güvenlik organizasyonu, erişim kontrolü, uyum, personel güvenliği, fiziki ve çevresel güvenlik, sistem bakım idamesi, iletişim ve işletim yönetimi, iş süreklik yönetimi olarak sınıflandırılmıştır (Vural& Sağıroğlu, 2008; Aydınlı, 2009).

BS–7799 ikinci kısmında kurumsal güvenlik ihtiyaçlarının belirlenmesi için gerekli olan bilgi güvenliği yönetiminin çatısı tanımlanarak BS–7799 birinci kısmında tanımlanan kontroller uygulanmaktadır. Bu standart, yöneticilere ve personele etkin bir BGYS kurmaları ve yönetmeleri açısından bir model sağlamak üzere hazırlanmıştır. Bu modelde "Planla– Uygula– Kontrol Et–Önlem Al (PUKÖ)" adımları bulunmaktadır.

Bilgi güvenliği yönetim sistemleriyle ilgili diğer bir İngiliz standardı Aralık 2005'te BS7799–3:2005 Bilgi Güvenliği Yönetim Sistemleri Risk Yönetiminin Kuralları ismiyle hazırlanmıştır. Standart 2006 yılında tekrar gözden geçirilmiş ve BS7799–3: 2006 ismiyle yayınlanmıştır. BS7799–3 standardı BS7799–2 standardının uygulanması için destek sağlayarak ölçeklenebilir (küçük, orta veya büyük kurumlar) yapıda standardın yaygınlaşmasına yardımcı olması için geliştirilmiştir. Standard içerisinde risk değerlendirmesi, belirlenen risklere kontrollerin uygulanması, tanımlanmış risklerin izlenmesi, kontrol yönetim sistemlerinin bakımı gibi risk yönetimi ile ilgili konular üzerine odaklanılmıştır. Kapsamın belirlenmesi, kural oluşturan kaynaklar, terimlerin tanımı, kurum bağlamında risk, risk değerlendirmesi, risk kararının verilmesi, risk yönetimi BS7799–3 standardının bölümlerini oluşturmaktadır (Vural & Sağıroğlu, 2008) .



Şekil: 6: BGYS Süreçlerine Uygulanan PUKÖ Modeli (Dinçkan & Öner, 2007).

Tablo 3: BGYS Süreçlerine Uygulanan PUKÖ Modeli (Dinçkan & Öner, 2007).

Planla **(BGYS'nin kurulması)**	BGYS politikası, amaçlar, hedefler, süreçler ve prosedürlerin geliştirilmesi
Uygula **(BGYS'nin gerçekleştirilmesi ve işletilmesi**	BGYS politikası, kontroller, süreçler ve prosedürlerin gerçekleştirilip işletilmesi
Kontrol Et **(BGYS'nin izlenmesi ve gözden geçirilmesi)**	BGYS politikası, amaçlar ve süreç performansının değerlendirilmesi, uygulanabilen yerlerde ölçülmesi ve sonuçların rapor edilmesi
Önlem Al **(BGYS'nin sürekliliğinin sağlanması ve iyileştirilmesi**	Yönetimin gözden geçirme sonuçlarına dayalı olarak, düzeltici ve önleyici faaliyetlerin gerçekleştirilmesi

2. ISO/IEC Standartları (ISO/IEC Standards)

Uluslararası Elektroteknik Komisyonunu (The International Electrotechnical Organization-IEC) 1906 yılında Uluslararası Standartlar Organizasyonu (International Organization for Standardization-ISO) 1947 yılında uluslararası alanda ticari (ISO) ve elektroteknik (IEC) standardizasyonun sağlanması için, İsviçre'nin Cenova şehrinde kurulmuştur. ISO ve IEC birlikte teknik çalışma grupları oluşturarak (Joint Technical Committee-JTC) tüm dünyada geçerli olacak standartlar oluşturmaktadırlar. Bununla birlikte ISO tarafından IT Güvenlik Standartları ile ilgili çalışmalar JTC–1 Bilişim Teknolojileri Komitesine bağlı SC27: BT Güvenlik Teknikleri Alt Komisyonunda ele alınmaktadır. Bilgi güvenliği konusunda çalışan bu komisyonun sorumluluklarından bazıları aşağıda belirtilmiştir. Bu sorumluluklar;

- Bilgi teknolojileri sistemleri güvenlik hizmetlerinin ve ihtiyaçların tanımlanması,
- Güvenlik teknikleri ve mekanizmalarının geliştirilmesi,
- Güvenlik kılavuzlarının geliştirilmesi ve
- Yönetim destek dokümanları ile standartların geliştirilmesidir.

ISO/IEC 17799 standardı: BS–7799 standardının ikinci sürümü Mayıs 1999'da çıktığında ISO, BSI'nın yayınladığı çalışmayla ilgilenmeye başlamıştır. Aralık 2000'de, ISO BS–7799 standardının ilk bölümünü alarak ISO/IEC 17779 olarak yeniden adlandırmış ve yeni bir standart olarak yayınlamıştır. ISO/IEC 17779 standardı daha önceki bölümde açıklanan BS–7799 standardının ilk bölümüne eşdeğerdir ISO/IEC 17799 standardının uygulanmasıyla kurumsal bilgilerin tamamen güvende olduğunu söylemek doğru değildir. Bu standart bilgi güvenliğini başlatan, gerçekleştiren ve sürekliliğini sağlayan kurumların kullanımı için, bilgi güvenlik yönetimi ile ilgili tavsiyeleri kapsar. ISO/IEC 17799 güvenlik standartlarını bir kurumun uyguluyor olması kurumlara aşağıda sıralanan üstünlükleri sağlamaktadır,

- Organizasyon Seviyesinde, sorumlulukları belirleyerek, kurumsal bilgi güvenliğinin her seviyede uygulanmasının yararlarını garanti eder.
- Kanuni Seviyede, kurumun ilgili tüm kural ve yönetmeliklere uyduğunu yetkili makamlara göstererek diğer standart ve mevzuatları tamamlar.
- İşletme Seviyesinde, Bilgi sistemleri, zafiyetleri ve nasıl korunacakları konusunda işletmenin yönlendirilmesini sağlayarak kurumsal bilgi sistemlerine daha güvenli erişim sağlanır.

- Ticari Seviyede, iş ortakları, hissedarlar ve müşteriler; kurumun bilgi koruması konusun verdiği önem sayesinde kuruma olan güvenleri artırır ve ticari rakipleri arasında piyasada farklı bir yere gelmesini sağlar.
- Finansal Seviyede, güvenlik açıklarının belirlenerek önlem alınması sonucunda maliyetler azalacaktır.
- Çalışan Seviyesinde, çalışanın güvenlik konuları ve organizasyon içinde kendisine düşen sorumluluk hakkındaki bilgisini arttırarak bireysel olarak bilinçlendirilmesini sağlar.

ISO/IEC 17799 standardı 2005 yılında gözden geçirilerek ISO/IEC 17799:2005 ismiyle son halini almıştır. ISO/IEC 17799:2005 Bilgi Güvenliği Yönetimi için uygulama kodu, kuruluşların bilgi güvenliği yönetim sistemini kurmaları, uygulamaları, sürdürmeleri ve iyileştirmeleri için hazırlanmış bir kılavuzdur. Önceki sürümünden farklı olarak, yaşanan problemlerden, arızalardan, kazalardan ders çıkarılması ve tekrar yaşanmaması için gerekli önlemlerin alınması için gerekli olan yönetim mekanizmasının kurulmasını sağlayan Bilgi Güvenliği İhlallerinin yönetimi ile ilgili bilgi güvenliği denetimlerini ve ilgili uygulamaları da içermektedir. ISO, 2005 yılında bir düzenlemeye giderek 27000 serisini bilgi güvenliği için kullanma kararı almıştır. ISO/IEC 27000-27059 arasındaki standartlar ISO tarafından SC27 grubuna dâhil çalışma grupları için bilgi güvenliğiyle ilgili planlanan standartlara ayrılmıştır. *ISO/IEC 27001,* BGYS için gereklilikleri ortaya koyan bir standarttır. Daha öncede anlatıldığı gibi bilgilerin düzenli olarak maruz kaldığı tehditlerin tanımlanmasına, yönetilmesine ve bunların minimize edilmesine yardımcı olur. Bu standart; yönetim standartlarıyla (ISO 9001, ISO 14001) uyumlu olarak geliştirildiğinden yönetim standartlarının gereklerini de yerine getirmektedir (Vural & Sağıroğlu, 2008).

Konuyla ilgili uluslararası düzenlemelerde 2008 yılında yayımlanan ve sağlık sektörü için bilgi güvenliği esaslarını bizlere sunan yeni ISO standardı; ISO 27799:2008 (Sağlık Bilgileri – Sağlıkta ISO/IEC 27002 bilgi güvenliği yönetimi) oldukça önemli. Bu standart son derece hassas olan kişisel sağlık bilgileri konusu ve bu bilgileri hem sağlık hizmetleri çalışanlarının erişiminin garanti edilmesi hem de gizliliğinin ve bütünlüğünün en iyi şekilde korunması konusunu değerlendirmekte ve bunu mümkün kılmak için bir hareket planı oluşturmaktadır. Sağlık bilgilerine her açıdan uygulanması öngörülen ISO 27799:2008, bilgilerin şekillendirilmesi, saklanması ve paylaşılması aşamasında gerekli olan tüm tedbirlerin alınması ve güvenlik altında

tutulması için detaylı standartlar da içermektedir. Aynı zamanda, ilgili Uluslararası Standartları uygulayarak, sağlık hizmetleri organizasyonları ve sağlık bilgileri koruyucularına boyutlarına ve durumuna göre gerekli görülen güvenlik şartlarını da sağlayabilmektedir (Hülür, 2009).

3. Türk Standartları (Turkish Standards)

Türkiye'de bilgi güvenliği standartlarıyla ilgili çalışmalar ve belgelendirmeler, Türk Standartları Enstitüsü (TSE) tarafından yapılmaktadır. TSE teknik kurulunun ISO/IEC 17799:2000 standardını tercüme ederek 11 Kasım 2002 tarihinde aldığı karar ile TS ISO/IEC 17799 Bilgi Teknolojisi-Bilgi Güvenliği Yönetimi İçin Uygulama Prensipleri Türk standardı olarak kabul edilmiştir. TS ISO/IEC 17799 standardı; kuruluşlar bünyesinde bilgi güvenliğini başlatan, gerçekleştiren ve süreklilik sağlayan, bilgi güvenliği yönetimi ile ilgili tavsiyeleri içermektedir. BGYS belgelendirilmesine yönelik TSE teknik kurulu tarafından yapılan çalışmalar sonucunda BS 7799– 2:2002 standardının tercümesi yapılarak "Bilgi Güvenliği Yönetim Sistemleri–Özellikler ve Kullanım Kılavuzu" ismiyle TS 17799–2 standardı olarak 17 Şubat 2005 tarihinde kabul edilmiş ve yürürlüğe girmiştir. Ancak TS ISO/IEC 27001:2006 "Bilgi Teknolojisi–Güvenlik Teknikleri-Bilgi Güvenliği Yönetim Sistemleri–Gereksinimler", 2.3.2006 tarihinde Türk standardı olarak kabul edildiğinden TS 17799–2 standardı TSE tarafından iptal edilmiştir. TS ISO/IEC 27001:2006 standardı, tüm kuruluş türlerini (örneğin, ticari kuruluşlar, kamu kurumları, kâr amaçlı olmayan kuruluşları) kapsar. Bu standart, bir BGYS'yi kuruluşun tüm ticari riskleri bağlamında kurmak, gerçekleştirmek, izlemek, gözden geçirmek, sürdürmek ve iyileştirmek için gereksinimleri kapsar. Bağımsız kuruluşların ya da tarafların ihtiyaçlarına göre özelleştirilmiş güvenlik kontrollerinin gerçekleştirilmesi için gereksinimleri belirtir. Bu standart ISO/IEC 27001:2005 standardından yararlanarak hazırlanmıştır. ISO/IEC 27001:2005 standardın tercümesidir(Vural &Sağıroğlu, 2008).

TABLO 4: Bilgi Güvenliği Yönetimini Destekleyen Standartlar ve Kılavuzlar (E-Dönüşüm, 2009).

Bileşen	Standart/Teknoloji	Açıklama
Bilgi güvenliği yönetimi için uygulama prensipleri	ISO/IEC 27002	Bilgi güvenliği yönetim sistemlerinde kullanılabilecek karşı önlem önerileridir. Mümkün olan hallerde milli olarak üretilen karşı önlemlerin kullanılmasına azami özen gösterilmelidir.
Bilgi güvenliği risk yönetimi için kılavuz	BS 7799-3:2006	BSI tarafından hazırlanmış olan kılavuzun orijinal ismi: Information security management systems. Guidelines for information security risk management
BGYS sertifikasyonu ihtiyaçları ve hazırlığı için kılavuz	-	BSI tarafından hazırlanmış olan kılavuzun orijinal ismi: Guidelines on Requirements and Preparation for ISMS Certification Based on ISO/IEC 27001
BGYS denetimine hazırlık kılavuzu	-	BSI tarafından hazırlanmış olan kılavuzun orijinal ismi: Are You Ready for an ISMSAudit Based on ISO/IEC 27001?
BGYS kontrollerinin uygulaması ve denetlemesi için kılavuzu	-	BSI tarafından hazırlanmış olan kılavuzun orijinal ismi:Guide to the Implementation and Auditing of ISMS Controls Based on ISO/IEC 27001
BGYS uygulamasının Etkinliğinin ölçülmesi kılavuz	-	BSI tarafından hazırlanmış olan kılavuzun orijinal ismi:Measuring theEffectiveness of your ISMS Implementations Based on ISO/IEC 27001

Bileşen	Standart/Teknoloji	Açıklama
Bilgi teknolojileri ve iletişim Teknolojilerinin güvenlik yönetimi için kavramlar ve modeller	ISO/IEC 13335-1:2004	ISO tarafından hazırlanmış olan standardın orijinal ismi:Information technology – Security techniques -- Management of informationand communications technology security -- Part 1: Concepts and models for information and communications technology security management
Bilgi teknolojileri güvenliğinin yönetimi için teknikler	ISO/IEC TR 13335-3:1998	ISO tarafından hazırlanmış olan standardın orijinal ismi:Guidelines for the management of IT Security -- Part 3: Techniques for themanagement of IT Security
Karşı önlemlerin seçimi	ISO/IEC TR 13335-4:2000	ISO tarafından hazırlanmış olanstandardın orijinal ismi:Guidelines for the management of IT Security -- Part 4: Selection of safeguards
Ağ güvenliği için yönetim kılavuzu	ISO/IEC TR 13335-5:2001	ISO tarafından hazırlanmış olanstandardın orijinal ismi:Information technology -- Guidelines forthe management of IT Security -- Part 5: Management guidance on network security
İş sürekliliği yönetimi için Uygulama prensipleri	BS 25999–1:2006	BSI tarafından hazırlanmış olanstandardın orijinal ismi:Code of practice for business continuity management

Bileşen	Standart/Teknoloji	Açıklama
Bilgi güvenliği yönetim sistemleri – Özellikler ve kullanım kılavuzu	TS ISO/IEC 27001	Kurumların dökümante edilmiş bir BGYS' yi tüm ticari riskleri bağlamında kurmak, gerçekleştirmek, izlemek, gözden geçirmek, bakımını yapmak ve iyileştirmek için gereksinimleri kapsar. Standart, ISO/IEC 27001:2005 standardının Türkçe çevirisidir
Bilgi güvenliği risk yönetimi için kılavuz	BS 7799-3:2006	BSI tarafından hazırlanmış olan kılavuzun orijinal ismi: Information security management systems. Guidelines for information security risk management
BGYS sertifikasyonu ihtiyaçları ve hazırlığı için kılavuz	-	BSI tarafından hazırlanmış olan kılavuzun orijinal ismi: Guidelines on Requirementsand Preparation for ISMS Certification Based on ISO/IEC 27001
BGYS denetimine hazırlık kılavuzu	-	BSI tarafından hazırlanmış olan kılavuzun orijinal ismi: Are You Ready for an ISMS Audit Based on ISO/IEC 27001?
BGYS kontrollerinin uygulaması ve denetlemesi için kılavuz	-	BSI tarafından hazırlanmış olan kılavuzun orijinal ismi:Guide to the Implementation and Auditing of ISMS Controls Based on ISO/IEC 27001
BGYS uygulamasının Etkinliğinin ölçülmesi kılavuzu	-	BSI tarafından hazırlanmış olan kılavuzun orijinal ismi: Measuring the Effectiveness of your ISMS Implementations Based on ISO/IEC 27001

Bileşen	Standart/Teknoloji	Açıklama
Bilgi teknolojileri ve iletişim Teknolojilerinin güvenlik yönetimi için kavramlar ve modeller	ISO/IEC 13335-1:2004	ISO tarafından hazırlanmış olan standardın orijinal ismi:Information technology – Security techniques -- Management of informationand communications technology security -- Part 1: Concepts and models for information and communications technology security management
Bilgi teknolojileri üvenliğinin yönetimi için teknikler	ISO/IEC TR 13335-3:1998	ISO tarafından hazırlanmış olan standardın orijinal ismi: Guidelines for the management of IT Security -- Part 3: Techniques for themanagement of IT Security
Karşı önlemlerin seçimi	ISO/IEC TR 13335-4:2000	ISO tarafından hazırlanmış olan standardın orijinal ismi:Guidelines for the management of IT Security -- Part 4: Selection of safeguards
Ağ güvenliği için yönetim kılavuzu	ISO/IEC TR 13335-5:2001	ISO tarafından hazırlanmış olan standardın orijinal ismi:Information technology -- Guidelines forthe management of IT Security -- Part 5: Management guidance on network security
İş sürekliliği yönetimi için Uygulama prensipleri	BS 25999–1:2006	BSI tarafından hazırlanmış olan standardın orijinal ismi: Code of practice for business continuity management

2.2.6. Sağlık İşletmelerinde Bilgi Güvenliği Kültürü Gelişim Süreci

Sağlık hizmetlerinin genel amacı; toplumun sağlık düzeyini yükseltmek ve devamlılığını sağlamaktır. Bu genel amaca bağlı sağlık hizmetlerinin amacı, hizmetin kapsayıcılığını, erişilebilirliğini, hakkaniyetini, etkinliğini yükseltmek ve gereksinimi olana kaliteli sağlık hizmeti sunabilmektir.

Günümüzde, hastanelerde yatarak tedavi gören hasta sayısındaki azalmaya karşın ayakta tedavi gören hasta sayısı önemli ölçüde artmıştır. Bu trend, birçok tıbbi prosedürün uygulama evresini geliştirerek hastaların iyileşme sürelerini düşüren tıbbi teknolojideki gelişimlerden büyük ölçüde etkilenmiştir. Sağlık bilişim güvenliği, bilgi üretimi ve bilgi teknolojilerinin yaygın kullanımı ile ciddi boyutlarda artmıştır. Sağlık bilişim teknolojileri kullanımının artması ile bilginin büyük çoğunluğu basılı dokümanlardan, bilgi teknolojileri tarafından işlenir hale dönüşmüştür. Buna paralel olarak sağlık işletmelerinde bilgiye erişim süreci ve hızı oldukça yüksektir. Bu durum, birçok avantajlarının yanı sıra dezavantajı da beraberinde getirmektedir. Sağlık bilgi teknolojileri üzerinde bilinçli veya bilinçsiz yapılan hatalar çok ciddi sonuçlar doğurabilir. Sağlık bilgi teknolojilerindeki açıklıklar ve dikkatsiz yapılandırmalar, bilgiye yetkisiz erişime yol açabilir. Bu durumda sağlıkla ilgili bilginin yetkisiz imhası ve değiştirilmesi söz konusu olabilir. Geçmişte sağlıkta bilgi güvenliği, sadece fiziksel güvenliğin tesis edilmesi ile sağlanırken, günümüzde kurumların en çok zorlandıkları öncelikli bir gereksinim gösteren konulardan biridir. Sağlık işletmeleri, diğer işletmeler gibi çevresinden farklı girdiler alıp bunları bir süreçten geçirip nihai olarak hayati bir öneme sahip hizmet sunarlar. Sağlık işletmelerinde dış çevre ve ürün yelpazesi karmaşıktır. Süreç açısından işlevler değişiktir. Sağlık sorunlarının çözümünde bazı hallerde geri bildirim mekanizması tam organize edilmek durumundadır. Sağlık işletmeleri, sağlık hizmetlerinin temel özelliği itibariyle tanı, teşhis tedavi başta olmak üzere işlevsel süreçlerin her evresinde yüksek bir güven faktörünün ön planda olduğu yapılardır. Modern sağlık hizmetleri katılımcılara anında, çabuk, tam ve doğru çözümler verebilmelidir. Çünkü tüm sağlık hizmetinin çok yönlü sunumunda katılımcıların etkin paylaşımcı katılım süreci söz konusudur. Bunun yanında sağlık hizmetlerinde hizmet alanlar/sunanların ihtiyaç ve farklı beklentileri her geçen gün değişmektedir. Sağlıkta gelişen yeni buluşlar ve çözümlerin yanında değişen tüm faktörlerin doktor/hastaya sağlıkta etik ilkeler ışığında birleştirilmesi gereklidir. Bunun için sağlık işletmesi, insan kaynağının faaliyetine başladıktan sonrada yenilikleri çok

yakından izlemelidir. Sağlık merkezlerinin tüm bu hızlı değişimleri anında takip edip cevap verebilmesi büyük bir önem taşır.

Sağlık işletmelerinde kurumsal bilgi güvenliği çalışmaları, hizmetin karakteristik özellikleri nedeni ile hizmet sektöründe yer alan diğer işletmelere göre daha farklı yaklaşımlar içerisinde sürdürülmektedir. Sağlık işletmelerinin karakteristik özellikleri şu şekilde sıralanabilir (Marşap & Akalp & Yeniman, 2010).

- Hastaneye gelen her hasta farklı tanı ve tedavi özellikleri göstermektedir. Belli bir zaman için hastaneye yönelen ya da yönelecek olan talep çoğu zaman doğru tahmin edilememektedir.
- Hastaneler talep değişikliğine kısa dönemde uyum sağlayamamaktadır.
- Hizmetin üretimi stoklanamamaktadır. Üretildiği anda tüketilmektedir.
- Sağlık işletmelerinde aşırı iş bölümü ve uzmanlaşma, nitelikli personel artışı ile beraber işgücü maliyetlerindeki artışı da getirmektedir.
- Her hastaya uygulanan sağlık hizmeti bileşiklik göstermesi hizmetin tanımlanmasını olanaksızlaştırmakta ve çıktıların standart olmasını engellemektedir. Sağlık hizmetlerinin özelliği, kesintisizlik, süreklilik, uzmanlık, kalite, iletişim ve değerlendirici süreç, sistemin teknik ve karmaşık yapısı, açık ve dinamik sistem özelliklerini taşır. Bu temel ilkelerin yanı sıra, sağlıkta bilişim teknolojilerinin sunduğu yeni olanakları kendi bünyesinde değişim sürecine uyumlu geçişler sağlayan model kalitesi, etkin zaman kullanımı ve gelişimi de beraberinde getirir. Sağlık bilişim potansiyelinin gerçekleştirmesini engelleyen riskli noktalar oluşabilir.

Temel işlerin yürütülmesi için bilgi, hayati bir kaynaktır. Göreceli olmakla birlikte, sağlık sektörü bilgiye dayalı iş sahalarının en önemlisidir. Büyük bir hızla artan tıp bilgisi ve buna paralel olarak çoğalan ve gelişen ölçü ve görüntüleme yöntemleri, giderek otomatikleşen tıbbi test, analiz ve izleme cihazları, bireyler ve hastalar için toplanılan veri ve bilgileri de büyük bir hızla arttırmaktadır. Daha iyi sağlık hizmeti üretebilmek için gerekli bilgi ve verilerin toplanması, kullanılması, paylaşılabilmesi ve bilgi üretiminin standart yöntemlerle gerçekleştirilmesi, üretilen bilgiden en üst düzeyde yararlanmayı sağlar (Çetin &Aydos, 2006).

Hizmet türlerinin ve rollerinin çeşitliliği nedeniyle sağlık hizmeti sunan kurumlarda, hizmet üretiminin ve üretim yönetiminin planlanmasında ihtiyaç duyulan bilgiye erişim, oldukça zor ve karmaşık bir süreç gerektirmektedir. Bu nedenle bilgi üretimi ve bilgiye erişim yöntemleri en baştan iyi bir şekilde tasarlanmalıdır. İdari ve mali kayıtların tutulması ve kullanılmasındaki başarılı uygulamaların, tıbbi kayıtların tutulması ve kullanılması bakımından da eşdeğer bir başarı çizgisine ulaşması gerekmektedir (Çetin & Aydos, 2006).

"Sağlık kayıtlarının güvenliği" ve "kişisel sağlık kayıtlarının mahremiyeti" konularının birbirinden bağımsız konular olmasının yanında hangi koşulda olursa olsun bu sağlık kayıtlarının güvenlik kriterlerine uygun olarak toplanması ve depolanması gerekmektedir (Çetin & Aydos, 2008). Sağlık kayıtlarının "güvenilirliği, mahremiyeti ve kişiselliği" sorunu aslında elektronik veriler oluşmadan önce de vardı. Sağlık bilgilerinin elektronik ortama aktarılması ve elektronik ortamda taşınması ile birlikte geçmişte fiziksel kısıtlılıklar nedeniyle daha sınırlı yaşanan güvenlik sorunları artarak yaşanmaya başladığı için sorun çok daha net algılandı ve gündeme oturdu. Özellikle İnternet ile birlikte giderek tekleşen bilgisayar ağları ve veritabanları, nitelikleri birbirinden farklı olmakla birlikte özde hep "kişi haklarına" yönelik ciddi saldırıları gündeme getirdi. Özellikle ABD'de devletin düzenleyici kurumları da kişisel hakların korunmasına yönelik çalışmalar yapıyorlar. Federal Ticaret Komisyonu FTC, Federal İletişim Komisyonu FCC, ve daha pek çok kamusal kuruluş da "kişisel mahremiyet"e ilişkin pek çok yasal düzenlemeye yer vermektedirler. Avrupa Birliği'nin de kişisel haklara ilişkin pek çok çalışması yayınlanmıştır. Genel anlamda kişisel mahremiyetin ötesinde; kişisel sağlık bilgilerinin mahremiyeti tüm dünyada ayrı bir başlık olarak da tartışılmaktadır. Kişisel tıbbi bilgiler özellikle insan kaynakları yöneticilerin ilgisini yoğun olarak çekmekte çalışanların performansı sağlık bilgileri ile ilişkilendirildiğinde etik anlamda ciddi sorunlar çıkmaktadır (Musoğlu, 2001). Bu koşullar sağlandıktan sonra söz konusu verilere kimlerin hangi erişim haklarıyla ve hangi seviyelerde erişeceği belirlenmelidir. Bu noktadan sonra kişisel sağlık kayıtlarının mahremiyeti konusu başlar ve erişim seviyeleri mahremiyetin sınırlarını belirler. Dolayısıyla bireyleri tanımlayan kişisel sağlık kayıtlarını barındıran veri alanlarına erişimin kısıtlanmış, yetkilerin de seviyelendirilmiş olması gerekir (Çetin & Aydos, 2006).

Hastane bilgi sistemleri, başlangıçta sadece doğru faturalama ve irsaliye yazılımı için gereksiniminden doğsa bile zamanla tüm hastane işlemlerini; hasta kimlik, tetkik, muayene

bilgilerinin kaydı, randevu verme, reçete ve rapor hazırlama, laboratuar sonuçlarının aktarımı, elektronik hasta kayıtları, stok takibi, yönetim raporları, kalite verilerinin irdelenmesini de kapsayan süreçlere dönüşmektedir (Rodoplu, 2006).

Hasta kaydı bilgisi kapsamına, hasta ile ilgili sözlü bilgi, yazılı bilgi, tıbbı müdahaleler, ön tanı, teşhisler, grafik imajları, fatura gibi konular girmektedir (07.10.2005 /veri güvenliği).

Hastanelerdeki hasta yoğunluğu beraberinde hizmet veren personel sayısı ve çeşitliliğini getirdiği gibi iş yoğunluğunun azaltılması için gerekli olan bilgisayar sayısını da artırmaktadır. Günlük olarak sayısı binlere ulaşan hastalar ile birlikte gerek hasta yakını ve hastane personeli gerekse taşınabilir bilgisayara sahip olma oranı %80'lere varan ilaç firması temsilcileri bir hastane ağının temel kullanıcılarını oluşturmaktadır. Tüm hastane ağları, bünyesinde hastalara ait gizli ya da özel bilgileri barındırmasının yanı sıra günlük olarak yüz binlerce TL'yi bulan para akışını içeren mali bilgileri de barındırmaktadır. Yüksek risk oranına sahip bu verilerin hastane içinden veya dışından oluşabilecek saldırılara karşı korunması için bir hastane ağı kapsamında 7 gün 24 saat temelinde durmaksızın çalışan, yüksek güvenilirlik gerektiren ve sürekli bilgi akışının devam ettiği bir otomasyon sistemine sahip olmak gerekmektedir(Çetin & Aydos, 2008).

Bilgi teknolojilerinin uygulanmasında, bilgi birikimi tamamlandıktan sonra, bu bilginin organizasyon içerisinde yönetim fonksiyonlarıyla paralel olarak yaygınlaşması gerekmektedir. Böylece şirkete değer yaratacak bilgi sadece teknolojik gereksinimlerden ve gelişmelerden yola çıkılarak yapılmayacak, işletme yapısına uygun bilgi sistemleri uygulamaları, güçlü proje yönetimi ve katılımcı bir yaklaşımla yönetimi, bilgi yönetimini sağlanmış olacaktır. Bu süreçte bilgisayar destekli veri tabanlarını oluşturan, ağlarla birbirine bağlayan, geribildirimleri (feedback) bilgi haline dönüştüren ve karar verme yetisine sahip olan insandır. Bundan dolayı insan bilgi yönetiminin en önemli kaynaklarındandır; entelektüel sermayesidir (Rodoplu, 2006).

Bilgi ve İletişim Teknolojileri (BİT) günlük yaşamlarında bilgi ağları ve hizmetlerinin kullanımına bağımlı hale gelen günümüz insanı için giderek daha önemli hale gelmektedir. Bilgi ve iletişim teknolojilerinin hızla gelişmesi ve tüm dünyada yayılması ile kamu ve özel kesim uygulamalarının elektronik ortama aktarılması insanoğlu için büyük yararlar sağlayan gelişmelerdir. Ancak bu gelişmelerin kötü niyetli bazı kişiler tarafından suiistimal edilmesi, siber ortamın tehdit, saldırı ve zarar verme gibi amaçlarla kullanılması ile siber saldırılar dolayısıyla

kişilerin ve ülkelerin gördüğü zararların büyük boyutlara ulaşması güvenlik anlayışında değişikliklere yol açmış ve bilgi güvenliği konusu bireylerin, kurumların, ülkelerin ve uluslararası kuruluşların en önemli gündem maddelerinden biri haline gelmiştir (Ulaşanoğlu & Yılmaz & Tekin, 2010).

Elektronik ortamlardaki bilgilerin geniş kitlelerin erişebileceği bir şekilde bulunması bu bilgilerin risk oranlarını çok daha fazla artmıştır. Yerel ve geniş alan ağlarını bünyesinde barındıran hastane ağlarında bilgi sistemi uygulamalarının yaygınlaşması veri ve bilgi güvenliği açısından bazı problemleri beraberinde getirmektedir. Bu ağlardaki veri ve bilgi taleplerinin her geçen gün artması gerek kişisel bilgilerin gerekse kurumsal bilgilerin gizlilik ve mahremiyeti açısından sakınca oluşturmaktadır. Özellikle hasta ve hastalık kayıtlarının gizlilik ve mahremiyeti önem arz etmektedir. Güvenliğin önemli bir bileşeni de; medikal kayıtta kimin hangi bilgilere ulaşacağına ilişkin yetkilendirmelerdir. Bu yüzden verilerin korunması ve bu verilere erişimde farklı kişilerin farklı erişim haklarına ve gerekliliklerine sahip olması önem arz etmektedir (Çetin & Aydos, 2008).

Bütün kişisel ve kurumsal bilgilerin (klinik, idari, mâli vb.) güvenliğinin sağlanması için aşağıda belirtilen hususlara dikkat edilmelidir.

• Veri güvenliği konusunda üç temel prensibin göz önüne alınması gerekmektedir. Bunlar; gizlilik, bütünlük ve erişilebilirliktir.

• Kurumda kimin hangi yetkilerle hangi verilere ulaşacağı çok iyi tanımlanmalıdır. Rol bazlı yetkilendirme yapılmalıdır ve yetkisiz kişilerin hastanın sağlık kayıtlarına erişmesi mümkün olmamalıdır.

• Sağlık kayıt bilgileri hastaya aittir. Yetkilendirilmiş çalışanlar ancak kendisine kayıtlı olan hastaların sağlık kayıtlarına erişebilmelidirler. Ancak hastanın yazılı onayı ile diğer sağlık çalışanları bu veriye erişebilirler.

• Hasta taburcu olmuş ise hiçbir kurum çalışanı hastanın sağlık kayıtlarına erişemez.

• Hastanın rızası olmadan hiçbir çalışan sözle de olsa hasta sağlık bilgilerini hastanın yakınları dışında üçüncü şahıslara ve kurumlara iletemez.

• Hasta sağlık bilgileri ticari amaçlı olarak da üçüncü şahıslara iletilemez. Hastanın kullandığı ilaçlar, diyet programları vs. buna dahildir.

• Hasta dosyasının bir kopyası hastaya teslim edilmelidir. Hiçbir hasta kaydı, elektronik veya kağıt ortamında [Bakanlığımızın bu konularda çıkardığı genelgeler hariç] hiçbir kuruma veya üçüncü şahıslara sözlü veya yazılı olarak teslim edilemez. Yürürlükteki genelgelere göre Hasta Sağlık bilgilerini Sosyal Güvence Kurumları (Bağkur, SSK, ES, GSS) elde edebilir. Özel sigorta kurumları hastanın sağlık bilgilerini elde edemez.

• Hastanın dosyasının izlenmemesi için gerekli tedbirler alınmalıdır. [Hasta dosyalarının gelişi güzel ortada bırakılmaması, bilgisayar ekranının başkalarınca okunabilecek şekilde bırakılmaması gibi]

• Telefon ile konuşurken hasta ile ilgili mahrem bilgilerin üçüncü şahısların eline geçmemesine azami özen göstermelidir.

• Bütün hasta sağlık kayıtları fiziksel olarak korunmuş mekânlarda saklanmalıdır.

• Elektronik hasta kayıtlarına internet ortamından erişim mümkün olmamalıdır.

• Hasta sağlık bilgileri bilginin üretildiği kurum tarafından veya Bakanlığımızın Bilgi Yönetim sistemleri tarafından araştırma, istatistik ve Karar Destek Sistemleri için kullanılabilir. Bu durumda hasta sağlık bilgisi hasta tanımlayıcısı ile ilişkilendirilemez (07.10.2005 /veri güvenliği).

Sağlık Bakanlığı, bilgi sistemlerinde bilgi sistemlerinde paylaşılan idari, mali ve klinik verilerin güvenliğinin ve iş devamlılığının sağlanması, güvenlik ihlalinden kaynaklanabilecek kanuni risklerin en aza indirilmesi, yatırımların ve kurumun itibarının korunması için bütün kurumlarında bilgi sistemlerinin güvenliğinin sağlanması konusunda standartlar belirlenmiştir. Bakanlığın "Bilgi Güvenliği Politikası", genel olarak; e-posta güvenliği, anti-virüs sistemleri, şifreleme gibi 23 ana başlık altında toplanan metot ve kurallardan oluşmaktadır. Ayrıca bilişim sistemlerinin fiziksel olarak nasıl korunacağına dair talimatlar da yayınlandı. Bakanlık, bütün

sağlık kurumlarına, firewall, saldırı tespit ve önleme sistemleri, anti-virüs gateway çözümleri, VPN çözümleri, yazılım güncelleme servisleri, sunucuların güvenliğinin sağlanması için alınması gereken önlemler, web filtreleme çözümleri, domain yapılarının oluşturulması denetleme ve izleme konularında zorunlu ve opsiyonel çözümler oluşturmaları talimatı vermiştir. Kimlik denetimi için güçlü mekanizmalar kullanılması yönündeki çalışmalar yapan Bakanlık aile hekimleri için sayısal imza ve kimlik denetiminde akıllı kartlar kullanılması çalışmalarını da sürdürmektedir. Hastanelerde bu sistemleri kullanmak üzere TUBİTAK-UEKAE ile çalışmalar yürüten Bakanlık, ISO/TSE 17799 bilgi güvenliği sertifikası alınmayı planlamaktadır (Yıldız, 2007).

Sistem güvenliğinin sağlamak için:

• Veriye erişirken dört temel prensibin gerçekleştirilmesi gerekmektedir. Bunlar: izlenebilirlik, kimlik sınama, güvenirlik ve inkar edilememedir.

• Sağlık kurumları bünyesinde hasta tanımlayıcı olarak T.C. Kimlik numarası baz alınacaktır. Veri tabanlarında hiçbir zaman hastalık tanısı ile T.C. kimlik numarası eşleşmeyecek, T.C. kimlik numarasından tek yönlü algoritma ile türetilmiş özel bir tanımlayıcı numara kullanılacaktır.

• Bilgi sistemlerinde güvenlik veriye erişim bazında olacaktır. Bunun için bu sistemin özellikle yazılım ve veritabanı erişim katmanlarında özel uygulamalar oluşturulacaktır.

Veriye erişecek kişiler aşağıdaki şekilde tanımlanmıştır.

- Hasta kendi verisine online olarak hiçbir zaman erişmemelidir.
- Bir Aile hekimi ancak kendisine kayıtlı olan hastaların elektronik sağlık kayıtlarına erişebilmelidir.
- Hastanedeki yetkilendirilmiş sağlık çalışanları ise, ancak hastanın giriş tarihinden, taburcu olana kadar geçen zaman içerisinde ve ancak hasta kendisi ile ilgili sağlık kayıtlarının erişimine yazılı olarak onay vermiş ise hastanın elektronik sağlık kayıtlarına erişebilirler. Ve bu da "geçici bir süreliğine" olacaktır.

• Sistem yöneticilerine de bir güvenlik katmanı konulacaktır. Bunun için veritabanı yazılımının gelişmiş güvenlik yönetimi özellikleri kullanılacaktır.

• Gerektiğinde saat ve/veya gün bazında belirlenen bir süre için bazı kullanıcı ve işlemci makinelerin sisteme oturum açmalarına kısıtlama getirilebilmelidir.

• Aynı kullanıcı kodu ile aynı anda birden fazla oturum açılmasına izin verilmemelidir.

• Eğer hasta, herhangi bir sağlık çalışanının elektronik sağlık kayıtlarına erişmesini istemiyorsa, sağlık çalışanı ilgili dosyayı okuma hakkına kavuşamamalıdır. Fakat sağlık çalışanı muayene sonuçlarını hastanın veri tabanına aktarabilmelidir. Bu diğer doktorlar tarafından yazılan kayıtlara erişilmemesi için kullanılan metottur.

• Sadece yetkisi olan kullanıcılar için veri girişi ve/veya verinin elde edilmesi için erişim izni verilmelidir. Birçok kullanıcının veri tabanında sadece belirli bir veri setine erişim yetkisinin denetlenebilmesini sağlamak için çok katmanlı denetim mekanizmaları olmalıdır.

• Veri tabanında tutulacak verilerin tutarlılığı tam ve kesin bir şekilde sağlanmalıdır.

Bunu sağlamak için en azından, veri onay (validation), çapraz sorgulama (crosschecking) ve mükerrer kayıt önleme gibi ölçütler uygulanmalıdır.

• Yönetimsel analizler yapmak için veri tabanındaki veriler bir yerden başka bir yere aktarılırken, kayıtlarda bulunan kişisel kimlik tanımlayıcıları kayıtlardan çıkartılmalı ve analizler hasta ile hastalık bilgilerini eşleştirmeden yapılmalıdır.

• Kullanıcı aktiviteleri (yapılan tüm işlemler ve erişimler) izlenebilmelidir. Veri tabanı üzerinde yapılan şüpheli işler denetlenebilmelidir. Sistemin hem etkin bir şekilde yönetilmesi, hem de yetkisiz erişimlerin engellenmesi ve izlenmesi anlamında gelişmiş bir kontrol mekanizması olmalıdır. Sistem, hangi kullanıcının sistemin hangi kısmına ne zaman ve nereden eriştiğine dair (zaman damgası-date stamp, işlem, kullanılan işlemci bilgisayar tanımı gibi bilgileri de içeren) kayıt tutmalıdır.

• Sistem yöneticilerinin kimlik tanımlama ve doğrulaması için X.509v3 uyumlu sayısal sertifikalar kullanılmalıdır. Sayısal sertifikaların güvenli depolaması için akıllı kartlar veya usb token cihazları kullanılmalıdır.

• Sertifika tabanlı kimlik doğrulama yapılmadığı halde password ve hash tabanlı kimlik doğrulama yapılacaktır. Sistemlere erişim için tek yönlü şifreleme algoritmaları kullanılacaktır.

• Kurum içerisinde veya Kurum ile başka ağlar arasındaki tüm haberleşme şifreli yapılmalıdır. Bütün iletişim VPN ve Açık Anahtar Alt Yapısı (PKI) teknolojilerini kullanmalıdır (07.10.2005 /veri güvenliği).

3. GEREÇ VE YÖNTEM

3.1. Araştırmanın Tipi

Bu araştırma, sağlık kuruluşlarında örgüt iklimi ve bilgi güvenliği ilişkisini belirlemek amacı ile tanımlayıcı araştırma türüne uygun olarak planlanmıştır.

3.2. Araştırmanın Yeri ve Zamanı

Araştırma, S.B. İzmir Bozyaka Eğitim ve Araştırma Hastanesi, S.B. İzmir Atatürk Eğitim ve Araştıma Hastanesi, S.B. İzmir Ege Doğumevi ve Kadın Hast. Eğit. ve Arş. Hastanesi, S.B. İzmir Dr. Suat Seren Göğüs Hast. ve Cer. Eğit. Arş. Hastanesi, S.B. Buca Seyfi Demirsoy Devlet Hastanesi, S.B. Buca Kadın Doğum ve Çocuk Hastalıklar Hastanesi, S.B. Karşıyaka Devlet Hastanesi, S.B. Nevval- Salih İşgören Alsancak Devlet Hastanesi, S.B. Dr. Ekrem Üstündağ Kadın Hst. Doğum Hastanesi, İzmir Özel Ege Tıp Hastanesi, İzmir Özel Tınaztepe Hastanesi, İzmir Özel Buca Tıp Hastanesi, İzmir Özel Kent Hastanesi'ndeki üst yönetime yapılmıştır. Başhekim/ Başhekim Yardımcısı, Başhemşire/ Başhemşire Yardımcısı, Müdür/ Müdür Yardımcısı, çalışmaya katılmaya gönüllü olmaktır. Araştırma 1 Nisan -1 Mayıs 2011 tarihlerinde yapılmıştır.

3.3. Araştırmanın Evreni ve Örneklemi

Araştırma 1 Nisan -1 Mayıs 2011 tarihleri arasında toplam 13 hastanedeki yöneticilere yapılaraktan 107 kişiye ulaşılmıştır. Çalışmaya dahil edilme kriterleri: yetişkin (18 yaş ve üzeri) olmak, yönetici görevinde bulunmak. (Başhekim/ Başhekim Yardımcısı, Başhemşire/ Başhemşire Yardımcısı, Müdür/ Müdür Yardımcısı), çalışmaya katılmaya gönüllü olmaktır. S.B. İzmir Bozyaka Eğitim ve Araştırma Hastanesinde 19 yöneticiden 15'ne, S.B. İzmir Atatürk Eğitim ve Araştıma Hastanesinde 21 yöneticiden 10'nuna, S.B. İzmir Ege Doğumevi ve Kadın Hast. Eğit. ve Arş. Hastanesinde 9 yöneticiden 6'sına, S.B. İzmir Dr. Suat Seren Göğüs Hast. ve Cer. Eğit. Arş. Hastanesinde 13 yöneticiden 10'nuna, S.B. Buca Seyfi Demirsoy Devlet Hastanesinde 17 yöneticiden 12'sine, S.B. Buca Kadın Doğum ve Çocuk Hastalıklar Hastanesinde 8 yöneticiden 8'ine, S.B. Karşıyaka Devlet Hastanesinde 18 yöneticiden 8'ine, S.B. Nevval- Salih İşgören Alsancak Devlet Hastanesinde 13 yöneticiden 9'una, S.B. Dr. Ekrem Üstündağ Kadın Hst. Doğum Hastanesinde 11 yöneticiden 8'ine, İzmir Özel Ege Tıp Hastanesinde 7 yöneticiden 7'sine , İzmir Özel Tınaztepe Hastanesinde 4 yöneticiden 4'üne, İzmir Özel Buca Tıp Hastanesinde 3 yöneticiden 3'üne, İzmir Özel Kent Hastanesinde 6 yöneticiden 6'sına ulaşılmıştır.

3.4.Araştırma Metaryali: Araştırmada kullanılan materyal yoktur.

3.5.Araştırma Değişkenleri: Araştırmanın bağımlı değişkeni "Örgüt İklimi", bağımsız değişkeni "Bilgi Güvenliği"dir.

3.6.Veri Toplama Araçları:

Araştırmada literatürden elde edilen bilgiler ışığında oluşturulan yapılandırılmış anket tekniği kullanılacaktır. Anket Robert Stringer tarafından geliştirilmiş örgüt iklimi ölçeği ve TS ISO 27799' dan çıkarılan bilgi güvenliği sorularından (EK-3) oluşmaktadır. Üç bölümden oluşan ankette toplam 61 soru bulunmaktadır. İlk bölümde örgütsel iklime yönelik 30 soru, ikinci bölümde bilgi güvenliği ile ilgili 26 soru son olarak da demografik değerlendirmelerin yer aldığı 7 soru bulunmaktadır. Ölçekte yer alan sorular beşli Likert ölçeğine göre derecelenmiştir. Örneğin: (1) Kesinlikle Katılmıyorum, (2) Katılmıyorum, (3) Ne Katılıyorum Ne Katılmıyorum, (4) Katılıyorum, (5) Kesinlikle Katılıyorum şeklinde derecelendirilmiştir.

3.7. Araştırma Planı ve Takvimi:

ZAMAN	YAPILANLAR
Eylül 2010-Aralık 2010	Literatür Tarama, Tez Önerisi Hazırlama
Ocak 2011	Veri Toplanacak Kurumlardan İzin Alınması
Mart 2011	Etik Kurul İzni
Nisan-Mayıs 2011	Verilerin Toplanması
Haziran 2011-Temmuz 2012	Verilerin Analizi ve Tartışmanın Yazılması

3.8. Verilerin Değerlendirilmesi:

Araştırma verileri SPSS 17.0 (Statistical Programme for Social Sciencies) programı ile analiz edilmiştir. Araştırma bulguları kapsamında katılımcıların sosyo-demografik özellikleri, geçerlilik ve güvenilirlik analizleri, örgüt iklimi ve bilgi güvenliğine yönelik tanımlayıcı istatistikler, t-testi, ANOVA testi ve korelasyon analizlerine yer verilmiştir.

3.9. Araştırmanın Sınırlılıkları: Araştırmayı çok sayıda hastanede yapılması ve yönetici grubuna ulaşmada zorluk yaşanmıştır.

3.10. Etik Kurul Onayı:

31.03.2011 tarihli ve 144-GOA protokol numaralı 2011/10-07 karar numaralı etik kurulu kararı Ek-1'de yer almaktadır.

4. BULGULAR

Araştırma Hipotezleri

H_1: Katılımcıların cinsiyetlerine göre örgüt iklimi değişkenlerine verdikleri yanıtlar arasında anlamlı bir farklılık vardır.

H_2: Katılımcıların yaşlarına göre örgüt iklimi değişkenlerine verdikleri yanıtlar arasında anlamlı bir farklılık vardır.

H_3: Katılımcıların eğitim durumlarına göre örgüt iklimi değişkenlerine verdikleri yanıtlar arasında anlamlı bir farklılık vardır.

H_4: Katılımcıların görevlerine göre örgüt iklimi değişkenlerine verdikleri yanıtlar arasında anlamlı bir farklılık vardır.

H_5: Katılımcıların toplam iş tecrübelerine göre örgüt iklimi değişkenlerine verdikleri yanıtlar arasında anlamlı bir farklılık vardır.

H_6: Katılımcıların mevcut işyerinde çalışma sürelerine göre örgüt iklimi değişkenlerine verdikleri yanıtlar arasında anlamlı bir farklılık vardır.

H_7: Örgüt iklimi değişkenleri arasında anlamlı bir ilişki vardır.

H_8: Katılımcıların cinsiyetlerine göre bilgi güvenliği değişkenlerine verdikleri yanıtlar arasında anlamlı bir farklılık vardır.

H_9: Katılımcıların yaşlarına göre bilgi güvenliği değişkenlerine verdikleri yanıtlar arasında anlamlı bir farklılık vardır.

H_{10}: Katılımcıların eğitim durumlarına göre bilgi güvenliği değişkenlerine verdikleri yanıtlar arasında anlamlı bir farklılık vardır.

H_{11}: Katılımcıların görevlerine göre bilgi güvenliği değişkenlerine verdikleri yanıtlar arasında anlamlı bir farklılık vardır.

H_{12}: Katılımcıların toplam iş tecrübelerine göre bilgi güvenliği değişkenlerine verdikleri yanıtlar arasında anlamlı bir farklılık vardır.

H_{13}: Katılımcıların mevcut işyerinde çalışma sürelerine göre bilgi güvenliği değişkenlerine verdikleri yanıtlar arasında anlamlı bir farklılık vardır.

H_{14}: Bilgi güvenliği değişkenleri arasında anlamlı bir ilişki vardır.

H_{15}: Örgüt iklimi ve bilgi güvenliği arasında anlamlı bir ilişki vardır.

ARAŞTIRMA BULGULARI

Araştırma bulguları kapsamında katılımcıların sosyo-demografik özellikleri, geçerlilik ve güvenilirlik analizleri, örgüt iklimi ve bilgi güvenliğine yönelik tanımlayıcı istatistikler, t-testi, ANOVA testi ve korelasyon analizlerine yer verilmiştir.

- **Katılımcıların Sosyo-Demografik Özellikleri**

Araştırma kapsamında katılımcılara cinsiyetleri, yaşları, eğitim durumları, görevleri, toplam iş tecrübeleri ve işyerindeki çalışma sürelerine ilişkin sorular yöneltilmiştir. Bu doğrultuda katılımcıların sosyo-demografik özelliklerine yönelik sayısal ve yüzdesel dağılımları Tablo 5'de ele alınmaktadır.

Katılımcıların sosyo-demografik özellikleri incelendiğinde araştırmaya katılanların %50,5'si kadın ve %49,5'i erkektir. Katılımcıların yaş dağılımları incelendiğinde %32,4'ünün 40 yaş ve altında, %47,6'sının 41-50 yaş arasında ve %20'sinin 51 yaş ve üzerinde olduğu görülmektedir. Katılımcıların %12,3'ü önlisans ve altında eğitim düzeyine, %46,2'si lisans eğitim düzeyine ve %41,5'i ise lisansüstü eğitim düzeyine sahip olduklarını belirtmişlerdir. Araştırmaya katılanların görev dağılımları incelendiğinde %33,7'sinin başhemşire veya başhemşire yardımcısı, %32,7'sinin başhekim veya başhekim yardımcısı ve %33,6'sının müdür veya müdür yardımcısı olduğu tespit edilmiştir.

Tablo 5: Katılımcıların Sosyo-Demografik Özelliklerine Göre Dağılımı

	N	%		N	%
Cinsiyet			***Görev***		
Kadın	53	50,5	Başhemşire/Başhemşire Yard.	35	33,7
Erkek	52	49,5	Başhekim/Başhekim Yard.	34	32,7
Toplam	**105**	**100,0**	Müdür/Müdür Yard.	35	33,6
Yaş Grupları			**Toplam**	**104**	**100,0**
40 yaş altı	34	32,4	**Toplam İş Tecrübesi**		
41-50 yaş arası	50	47,6	10 yıldan az	17	16,3
51 yaş ve üzeri	21	20,0	10 yıldan fazla	87	83,7
Toplam	**105**	**100,0**	**Toplam**	**104**	**100,0**
Eğitim Durumu			**İşyerindeki çalışma süresi**		
Önlisans ve altı	13	12,3	5 yıl ve altı	29	27,6
Lisans	49	46,2	6-10 yıl arasında	29	27,6
Lisans üstü	44	41,5	11 yıl ve üzeri	47	44,8
Toplam	**106**	**100,0**	**Toplam**	**105**	**100,0**

Katılımcıların %16,3'ü 10 yıl ve daha az toplam iş tecrübesi ve %83,7'si ise 10 yıldan daha fazla toplam iş tecrübesi olduklarını belirtmişlerdir. Katılımcıların işyerindeki çalışma süreleri incelendiğinde ise, %27,6'sı 5 yıl ve daha az süredir çalıştığını, %27,6'sı 6 yıl ile 10 yıl arasında çalıştıklarını ve %44,8'i 11 yıl ve üzerinde çalıştıklarını belirtmişlerdir. Araştırma gerçekleştirilen hastaneler, hastanelerden toplanan anket sayıları ve yüzdesel dağılımları Tablo 6'da ele alınmaktadır.

Tablo 6: Araştırma Gerçekleştirilen Hastanelerin Dağılımı

	N	***%***
2	7	6,6
3	8	7,5
4	12	11,3
5	8	7,5
6	15	14,2
7	10	9,4
8	9	8,5
9	7	6,6
10	8	7,5
11	6	5,7
12	6	5,7
13	10	9,4
Toplam	**106**	**100,0**

- **Geçerlilik ve Güvenilirlik Analizi**

Örgüt İklimi veri seti daha önce Robert Stringer tarafından uygulanmış ve geçerliliği kanıtlanmıştır. Örgüt iklimi veri setine gerçekleştirilen güvenilirlik analizi sonucunda ise genel Cronbach Alpha değeri 0,90 ($p<0,001$) olarak tespit edilmiştir.

Bilgi güvenliği veri seti ilk defa oluşturulduğu ve uygulandığından hem içerik hem de yapısal geçerliliği sınanmıştır. Gerçekleştirilen faktör analizi Tablo 7'de ele alınmaktadır. Geçerlilik analizi sonrasında bilgi güvenliği veri setine güvenilirlik analizi gerçekleştirilmiştir. Güvenilirlik analizi sonucunda genel Cronbach Alpha değeri 0,94 ($p<0,001$) olarak tespit edilmiştir.

Tablo 7: Faktör Analizi (Bilgi Güvenliği)

	Faktör Yükü	Özdeğerler	Açıklanan Varyans Yüzdesi	M	F Değeri	Alpha	P
1. FAKTÖR - BİLGİ GÜVENLİĞİ YÖNETİMİ		10,448	41,793	3,99	6,169	,91	<,001
Bilgi sistemleri edinmenin kuralları bulunmaktadır.	,869						
Bilgi güvenliği güvenlik olayları etkili bir şekilde sonuçlanır.	,864						
Kişisel sağlık bilgileri şifreli bir formatta tutulmaktadır.	,768						
Acil durumlarda erişim kontrol kuralları belirlidir.	,752						
Bilgi güvenliği yönetim sistemi sağlıklı uygulanmaktadır.	,709						
Kurumdan ayrılan personelin kullanıcı erişim yetkileri hemen iptal edilir.	,604						
Kurumuzda bilgi güvenliği uygulamasında yönetim kararlıdır.	,567						
2. FAKTÖR- BİLGİ GÜVENLİĞİ YAKLAŞIMI		2,590	10,358	3,92	2,599	,87	,052
Bilgi güvenliği sorumluları belirlidir.	,719						
Bilgi güvenliği politikası bulunmaktadır.	,711						
Kurumumuzda fiziksel ve çevresel güvenlik sağlanmaktadır.	,655						
Kişisel sağlık verilerini korumak için kurallar bulunmaktadır.	,582						

	Faktör Yükü	Özdeğerler	Açıklanan Varyans Yüzdesi	M	F Değeri	Alpha	P
3. FAKTÖR – BİLGİ GÜVENLİĞİ UYGULAMASI		2,069	8,276	3,46	6,813	,85	<,001
Sistematik risk yönetimi uygulaması bulunmaktadır.	,817						
Benzer kurumlarla bilgi güvenliği kıyaslaması yapılmaktadır.	,785						
Bilgi güvenliği iç denetimi yapılmaktadır.	,761						
Bilgi güvenliği komitesi bulunmaktadır.	,713						
Yönetim kaynakları etkin bir şekilde kullanır.	,630						
4. FAKTÖR- BİLGİ GÜVENLİĞİ KÜLTÜRÜ		1,317	5,266	3,86	6,032	,86	<,001
Sağlık bilgi güvenliğindeki tehditler ve güvenlik açıklıkları nettir.	,845						
Korunacak sağlık bilgileri belirlenmiştir.	,613						
Kurumsal bilgi güvenliği yönetim sistemi oluşturulmuştur.	,607						
Kurumuzda bilgi güvenliği hedefleri belirlenmiştir.	,579						
Kurumsal bilgi güvenliği klinik bazında izlenmektedir.	,497						
5. FAKTÖR- BİLGİ GÜVENLİĞİNDE GİZLİLİK		1,099	4,394	4,21	1,984	,66	,140
Kişisel sağlık bilgilerinin korunması gerekli değildir.	,804						

	Faktör Yükü	Özdeğerler	Açıklanan Varyans Yüzdesi	M	F Değeri	Alpha	P
Kendi sağlık bilgilerimin arkadaşlarım tarafından görülmesini isterim.	,759						
Tüm kişisel sağlık verileri gizli tutulmalıdır.	,740						
Kaiser-Meyer-Olkin Örneklem Ölçümü: ,873; Barlett's Test of Sphericity=1643,382 (p<0,001) Açıklanan Toplam Varyans: 70,088							

Bilgi güvenliği veri setinin yapısal geçerliliğini kanıtlamak amacıyla faktör analizi gerçekleştirilmiştir. Faktör analizi sonucunda Kaiser-Meyer-Olkin örneklem değeri 0,87 (p<0,001) olarak gerçekleşmiş ve açıklanan toplam varyans 70,09 olarak tespit edilmiştir. Tablo 7'de bilgi güvenliği veri setinin beş boyut altında oluştuğu görülmektedir.

İlk faktörün tanımladığı fark yüzdesi 41,79'dur ve 8 değişkenle ifade edilmektedir. Bu faktörün altında bulunan ifadeler incelendiğinde değişkenlerin "Bilgi Güvenliği Yönetimi" ile ilgili olduğu anlaşılmaktadır ve özdeğeri 10,45'tir. Bu faktöre göre anketi dolduranlar ortalama değer olarak 3,99 vermişlerdir.

İkinci faktörün tanımladığı fark yüzdesi 10,36'dır ve 4 değişkenle ifade edilmektedir. Bu faktörün altında bulunan ifadeler incelendiğinde değişkenlerin "Bilgi Güvenliği Yaklaşımı" ile ilgili olduğu anlaşılmaktadır ve özdeğeri 2,59'dur. Bu faktöre göre anketi dolduranlar ortalama değer olarak 3,92 vermişlerdir.

Üçüncü faktörün tanımladığı fark yüzdesi 8,28'dır ve 5 değişkenle ifade edilmektedir. Bu faktörün altında bulunan ifadeler incelendiğinde değişkenlerin "Bilgi Güvenliği Uygulaması" ile ilgili olduğu anlaşılmaktadır ve özdeğeri 2,07'dir. Bu faktöre göre anketi dolduranlar ortalama değer olarak 3,46 vermişlerdir.

Dördüncü faktörün tanımladığı fark yüzdesi 5,27'dir ve 5 değişkenle ifade edilmektedir. Bu faktörün altında bulunan ifadeler incelendiğinde değişkenlerin "Bilgi Güvenliği Kültürü" ile ilgili olduğu anlaşılmaktadır ve özdeğeri 1,32'dir. Bu faktöre göre anketi dolduranlar ortalama değer olarak 3,86 vermişlerdir.

Son olarak, beşinci faktörün tanımladığı fark yüzdesi 4,39'dur ve 3 değişkenle ifade edilmektedir. Bu faktörün altında bulunan ifadeler incelendiğinde değişkenlerin "Bilgi Güvenliğinde Gizlilik" ile ilgili olduğu anlaşılmaktadır ve özdeğeri 1,10'dur. Bu faktöre göre anketi dolduranlar ortalama değer olarak 4,21 vermişlerdir.

- **Örgüt İklimine İlişkin Bulgular**

Örgüt iklimi değişkenlerinin tanımlayıcı istatistikleri, katılımcıların demografik özelliklerine göre verdikleri yanıtlar arasında anlamlı bir farklılığın olup olmadığını tespit etmek amacıyla çeşitli analizler gerçekleştirilmiştir.

Tablo 8: Tanımlayıcı İstatistikler (Örgüt İklimi)

	N	Minimum	Maksimum	Ortalama	Standart Sapma
Organizasyon Yapısı	106	2,00	4,86	3,4180	,65537
Bireysel Sorumluluk	106	1,00	5,00	3,4819	,64979
Ödüllendirme	106	1,60	4,00	2,9807	,54984
Risk Alma	106	1,00	5,00	3,5236	,81176
Ilımlı Çalışma Ortamı	106	1,00	5,00	3,5236	,81176
Destek	106	1,00	4,80	3,3851	,80263

Örgüt iklimi değişkenleri olan "Organizasyon Yapısı", "Bireysel Sorumluluk", "Ödüllendirme", "Risk Alma", "Ilımlı Çalışma Ortamı" ve "Destek" faktörlerine verdikleri yanıtların ortalaması, standart sapmaları, minimum ve maksimum değerleri Tablo 8'de ele alınmıştır. Örgüt iklimi değişkenlerinden "Risk Alma" ve "Ilımlı Çalışma Ortamı" en yüksek ortalamaya ve "Ödüllendirme" ise en düşük ortalamaya sahiptir.

Tablo 9: Cinsiyete Göre Verilen Yanıtlar

	Cinsiyet	N	Ortalama	Std. Sapma	t	p
Ödüllendirme	**Kadın**	53	3,1403	,53507	2,991	**,003**
	Erkek	52	2,8321	,52064		
Destek	**Kadın**	53	3,5447	,65067	2,003	,048
	Erkek	52	3,2337	,91548		

Katılımcıların cinsiyetlerine göre örgüt iklimi değişkenlerine verdikleri yanıtlar arasında anlamlı bir farklılığın olup olmadığını tespit etmek amacıyla t testi gerçekleştirilmiştir. Tablo 9'da t testi sonucuna göre katılımcıların "Ödüllendirme" ve "Destek" değişkenleri için anlamlı bir farklılık tespit edildiği görülmektedir. Bu doğrultuda "Ödüllendirme" değişkeni için kadınların verdikleri yanıtların ortalaması 3,14 ve erkeklerin verdikleri yanıtların ortalaması 2,83'tür. "Destek" değişkeni için kadınların verdikleri yanıtların ortalaması 3,54 ve erkeklerin verdikleri yanıtların ortalaması 3,23'tür. Bu doğrultuda, H_1 "Ödüllendirme" ve "Destek" değişkenleri için kabul edilmiştir.

Katılımcıların yaşlarına göre örgüt iklimi değişkenlerine verdikleri yanıtlar arasındaki farklılığın olup olmadığını tespit edebilmek amacıyla ANOVA testi gerçekleştirilmiştir. Elde edilen bulgulara göre katılımcıların yaşlarına göre örgüt iklimi değişkenlerine verdikleri yanıtlar arasında anlamlı farklılık tespit edilememiştir. Bu doğrultuda H_2 reddedilmiştir.

Katılımcıların eğitim durumlarına göre örgüt iklimi değişkenlerine verdikleri yanıtlar arasındaki farklılığın olup olmadığını tespit edebilmek amacıyla ANOVA testi gerçekleştirilmiştir. Elde edilen bulgulara göre katılımcıların eğitim durumlarına göre örgüt iklimi değişkenlerine verdikleri yanıtlar arasında anlamlı farklılık tespit edilememiştir. Bu doğrultuda H_3 reddedilmiştir.

Tablo 10: Katılımcıların Görevlerine Göre Verilen Yanıtlar

	Görev	N	Ortalama	Std. Sapma	t	p
Ödüllendirme	Başhemşire/Başhemşire Yardımcısı	35	3,2048	,53328	6,617	,002
	Başhekim/Başhekim Yardımcısı	34	3,0029	,44709		
	Müdür/Müdür Yardımcısı	35	2,7576	,55630		
	Toplam	104	2,9883	,54235		
Destek	Başhemşire/Başhemşire Yardımcısı	35	3,6419	,69528	4,023	,021
	Başhekim/Başhekim Yardımcısı	34	3,4456	,80588		
	Müdür/Müdür Yardımcısı	35	3,1257	,80013		
	Toplam	104	3,4040	,79063		

Katılımcıların görevlerine göre örgüt iklimi değişkenlerine verdikleri yanıtlarda anlamlı bir farklılığın olup olmadığını tespit edebilmek amacıyla ANOVA testi gerçekleştirilmiştir. ANOVA testi sonucuna göre katılımcıların görevlerine göre "Ödüllendirme" ve "Destek" değişkenlerine verdikleri yanıtlarda anlamlı bir farklılık tespit edilmiştir. Bulgular Tablo 10'da ele alınmaktadır.

Bu doğrultuda "Ödüllendirme" değişkeni için başhemşire veya başhemşire yardımcılarının verdikleri yanıtların ortalaması 3,21, başhekim veya başhekim yardımcılarının verdikleri yanıtların ortalaması 3,00 ve müdür veya müdür yardımcılarının verdikleri yanıtların ortalaması 2,769'dır. "Destek" değişkeni için başhemşire veya başhemşire yardımcılarının verdikleri yanıtların ortalaması 3,64, başhekim veya başhekim yardımcılarının verdikleri yanıtların ortalaması 3,45 ve müdür veya müdür yardımcılarının verdikleri yanıtların ortalaması 2,13'tür. Bu doğrultuda, H_4 "Ödüllendirme" ve "Destek" değişkenleri için kabul edilmiştir.

Hangi gruplar arasında farklılığın olduğunu tespit etmek amacıyla yapılan Post Hoc Testlerinden LSD analizi Tablo 11'de gösterilmektedir. Bu analize göre "Ödüllendirme" değişkeni için başhemşire veya başhemşire yardımcılarının verdikleri yanıtlar ile müdür veya müdür yardımcılarının verdikleri yanıtlar arasında anlamlı bir farklılığın olduğu gözlenmektedir

(p<0,001). "Destek" değişkeni için başhemşire veya başhemşire yardımcılarının verdikleri yanıtlar ile müdür veya müdür yardımcılarının verdikleri yanıtlar arasında anlamlı bir farklılığın olduğu gözlenmektedir (p=0,006).

Katılımcıların toplam iş tecrübelerine göre örgüt iklimi değişkenlerine verdikleri yanıtlar arasındaki farklılığın olup olmadığını tespit edebilmek amacıyla t testi gerçekleştirilmiştir. Elde edilen bulgulara göre katılımcıların toplam iş tecrübelerine göre örgüt iklimi değişkenlerine verdikleri yanıtlar arasında anlamlı farklılık tespit edilememiştir. Bu doğrultuda H_5 reddedilmiştir.

Tablo 11: Katılımcıların Görevlerine İlişkin LSD Testi

LSD				
	(I)	(J)	Ortalama Farkları (I-J)	**P**
Ödüllendirme	Başhemşire/Başhemşire Yardımcısı	Başhekim/Başhekim Yardımcısı	,20182	,107
		Müdür/Müdür Yardımcısı	,44714*	**,000**
	Başhekim/Başhekim Yardımcısı	Başhemşire/Başhemşire Yardımcısı	-,20182	,107
		Müdür/Müdür Yardımcısı	,24532	,051
	Müdür/Müdür Yardımcısı	Başhemşire/Başhemşire Yardımcısı	-,44714*	**,000**
		Başhekim/Başhekim Yardımcısı	-,24532	,051
Destek	Başhemşire/Başhemşire Yardımcısı	Başhekim/Başhekim Yardımcısı	,19632	,291
		Müdür/Müdür Yardımcısı	,51619*	**,006**
	Başhekim/Başhekim Yardımcısı	Başhemşire/Başhemşire Yardımcısı	-,19632	,291
		Müdür/Müdür Yardımcısı	,31987	,087
	Müdür/Müdür Yardımcısı	Başhemşire/Başhemşire Yardımcısı	-,51619*	**,006**
		Başhekim/Başhekim Yardımcısı	-,31987	,087

Katılımcıların mevcut işyerlerinde çalışma sürelerine göre örgüt iklimi değişkenlerine verdikleri yanıtlar arasındaki farklılığın olup olmadığını tespit edebilmek amacıyla ANOVA testi gerçekleştirilmiştir. Elde edilen bulgulara göre katılımcıların mevcut işyerlerinde çalışma sürelerine göre örgüt iklimi değişkenlerine verdikleri yanıtlar arasında anlamlı farklılık tespit edilememiştir. Bu doğrultuda H_6 reddedilmiştir.

Tablo 12: Korelasyon Analizi (Örgüt İklimi)

		Organizasyon Yapısı	**Bireysel Sorumluluk**	**Ödüllendirme**	**Risk Alma**	**Ilımlı Çalışma Ortamı**	**Destek**
Organizasyon Yapısı	r	1					
	Sig.						
	N	106					
Bireysel Sorumluluk	r	,529	1				
	Sig.	,000					
	N	106	106				
Ödüllendirme	r	,590	,438	1			
	Sig.	,000	,000				
	N	106	106	106			
Risk Alma	r	,504	,503	,491	1		
	Sig.	,000	,000	,000			
	N	106	106	106	106		
Ilımlı Çalışma Ortamı	r	,504	,503	,491	1,000	1	
	Sig.	,000	,000	,000	,000		
	N	106	106	106	106	106	
Destek	r	,701	,538	,689	,648	,648	1
	Sig.	,000	,000	,000	,000	,000	
	N	106	106	106	106	106	106

Tablo 12'de de görüldüğü gibi "Organizasyon Yapısı" değişkeni ile "Bireysel Sorumluluk" değişkeni arasında pozitif yönde güçlü kuvvette bir ilişki ($p<0,001$ ve $r= 0,529$) olduğu görülmektedir. "Organizasyon Yapısı" değişkeni ile "Ödüllendirme" değişkeni arasında pozitif yönde güçlü kuvvette bir ilişki ($p<0,001$ ve $r= 0,590$) vardır. "Organizasyon Yapısı" değişkeni ile "Risk Alma" değişkeni arasında pozitif yönde güçlü kuvvette bir ilişki ($p<0,001$ ve $r= 0,504$) vardır. "Organizasyon Yapısı" değişkeni ile "Ilımlı Çalışma Ortamı" değişkeni arasında pozitif yönde güçlü kuvvette bir ilişki ($p<0,001$ ve $r= 0,504$) vardır. "Organizasyon Yapısı" değişkeni ile "Destek" değişkeni arasında pozitif yönde çok güçlü kuvvette bir ilişki ($p<0,001$ ve $r= 0,701$) vardır.

"Bireysel Sorumluluk" değişkeni ile "Ödüllendirme" değişkeni arasında pozitif yönde orta kuvvette bir ilişki ($p<0,001$ ve $r= 0,438$) vardır. "Bireysel Sorumluluk" değişkeni ile "Risk Alma" değişkeni arasında pozitif yönde güçlü kuvvette bir ilişki ($p<0,001$ ve $r= 0,503$) vardır. "Bireysel Sorumluluk" değişkeni ile "Ilımlı Çalışma Ortamı" değişkeni arasında pozitif yönde güçlü kuvvette bir ilişki ($p<0,001$ ve $r= 0,503$) vardır. "Bireysel Sorumluluk" değişkeni ile "Destek" değişkeni arasında pozitif yönde güçlü kuvvette bir ilişki ($p<0,001$ ve $r= 0,538$) olduğu tespit edilmiştir.

"Ödüllendirme" değişkeni ile "Risk Alma" değişkeni arasında pozitif yönde orta kuvvette bir ilişki ($p<0,001$ ve $r= 0,491$) vardır. "Ödüllendirme" değişkeni ile "Ilımlı Çalışma Ortamı" değişkeni arasında pozitif yönde orta kuvvette bir ilişki ($p<0,001$ ve $r= 0,491$) vardır. "Ödüllendirme" değişkeni ile "Destek" değişkeni arasında pozitif yönde güçlü kuvvette bir ilişki ($p<0,001$ ve $r= 0,689$) vardır. "Risk Alma" değişkeni ile "Ilımlı Çalışma Ortamı" değişkeni arasında pozitif yönde çok güçlü kuvvette bir ilişki ($p<0,001$ ve $r= 1,000$) vardır. "Risk Alma" değişkeni ile "Destek" değişkeni arasında pozitif yönde güçlü kuvvette bir ilişki ($p<0,001$ ve $r= 0,648$) olduğu görülmektedir. "Ilımlı Çalışma Ortamı" değişkeni ile "Destek" değişkeni arasında pozitif yönde güçlü kuvvette bir ilişki ($p<0,001$ ve $r= 0,648$) olduğu görülmektedir. Korelasyon analizinden elde edilen bulgulara göre H_7 kabul edilmiştir.

- **Bilgi Güvenliğine İlişkin Bulgular**

Katılımcıların bilgi güvenliği değişkenleri olan "Bilgi Güvenliği Yönetimi", "Bilgi Güvenliği Yaklaşımı", "Bilgi Güvenliği Uygulaması", "Bilgi Güvenliği Kültürü" ve "Bilgi Güvenliğinde Gizlilik" faktörlerine verdikleri yanıtların ortalaması, standart sapmaları, minimum ve maksimum değerleri Tablo 13'de ele alınmıştır. Bilgi güvenliği değişkenlerinden "Bilgi Güvenliğinde Gizlilik" en yüksek ortalamaya ve "Bilgi Güvenliği Uygulaması" ise en düşük ortalamaya sahiptir.

Tablo 13: Tanımlayıcı İstatistikler (Bilgi Güvenliği)

	N	Minimum	Maksimum	Ortalama	Standart Sapma
Bilgi Güvenliği Yönetimi	104	1,88	5,00	3,9892	,65176
Bilgi Güvenliği Yaklaşımı	104	1,50	5,00	3,9046	,78633
Bilgi Güvenliği Uygulaması	104	1,20	5,00	3,4726	,82397
Bilgi Güvenliği Kültürü	103	2,00	5,00	3,8466	,68597
Bilgi Güvenliğinde Gizlilik	104	1,67	5,00	4,2163	,72439

Tanımlayıcı istatistiklerden sonra katılımcıların cinsiyetlerine göre bilgi güvenliği değişkenlerine verdikleri yanıtlar arasındaki farklılığın olup olmadığını tespit edebilmek amacıyla t testi gerçekleştirilmiştir. Elde edilen bulgulara göre katılımcıların cinsiyetlerine göre bilgi güvenliği değişkenlerine verdikleri yanıtlar arasında anlamlı farklılık tespit edilememiştir. Bu doğrultuda H_8 reddedilmiştir.

Katılımcıların yaşlarına göre bilgi güvenliği değişkenlerine verdikleri yanıtlar arasındaki farklılığın olup olmadığını tespit edebilmek amacıyla ANOVA testi gerçekleştirilmiştir. Elde edilen bulgulara göre katılımcıların yaşlarına göre bilgi güvenliği değişkenlerine verdikleri yanıtlar arasında anlamlı farklılık tespit edilememiştir. Bu doğrultuda H_9 reddedilmiştir.

Tablo 14: Katılımcıların Eğitim Durumlarına Göre Verilen Yanıtlar

	Eğitim Durumu	**N**	**Ortalama**	**Std. Sapma**	**t**	**p**
Bilgi Güvenliğinde Gizlilik	Önlisans ve altı	13	3,7949	1,07616	5,404	,006
	Lisans	47	4,1135	,67128		
	Lisans üstü	44	4,4508	,57464		
	Toplam	104	4,2163	,72439		

Katılımcıların eğitim durumlarına göre bilgi güvenliği değişkenlerine verdikleri yanıtlarda anlamlı bir farklılığın olup olmadığını tespit edebilmek amacıyla ANOVA testi gerçekleştirilmiştir. ANOVA testi sonucuna göre katılımcıların eğitim durumlarına göre "Bilgi Güvenliğinde Gizlilik" değişkenine verdikleri yanıtlarda anlamlı bir farklılık tespit edilmiştir. Bulgular Tablo 14'de ele alınmaktadır.

Bu doğrultuda "Bilgi Güvenliğinde Gizlilik" değişkeni için önlisans ve altı eğitim düzeyine sahip olan katılımcıların verdikleri yanıtların ortalaması 3,80, lisans mezunu olan katılımcıların verdikleri yanıtların ortalaması 4,11 ve lisans ve üzerinde eğitim düzeyine sahip katılımcıların verdikleri yanıtların ortalaması 4,45'tir. Bu doğrultuda, H_{10} "Bilgi Güvenliğinde Gizlilik" değişkeni için kabul edilmiştir.

Tablo 15: Katılımcıların Eğitim Durumlarına İlişkin LSD Testi

LSD				
	(I)	(J)	Ortalama Farkları (I-J)	**p**
Bilgi Güvenliğinde Gizlilik	Önlisans ve altı	Lisans	-,31860	,147
		Lisans üstü	-,65589*	**,004**
	Lisans	Önlisans ve altı	,31860	,147
		Lisans üstü	-,33728*	**,023**
	Lisans üstü	Önlisans ve altı	,65589*	**,004**
		Lisans	,33728*	**,023**

Hangi gruplar arasında farklılığın olduğunu tespit etmek amacıyla yapılan Post Hoc Testlerinden LSD analizi Tablo 15'de gösterilmektedir. Bu analize göre "Bilgi Güvenliğinde Gizlilik" değişkeni için lisansüstü eğitim düzeyine sahip katılımcıların verdikleri yanıtlar ile önlisans ve altı eğitim düzeyine sahip katılımcıların verdikleri yanıtlar (p=0,004) ve lisans mezunu olan katılımcıların verdikler yanıtlar (p=0,023) arasında anlamlı bir farklılığın olduğu gözlenmektedir.

Katılımcıların görevlerine göre bilgi güvenliği değişkenlerine verdikleri yanıtlar arasındaki farklılığın olup olmadığını tespit edebilmek amacıyla ANOVA testi gerçekleştirilmiştir. Elde edilen bulgulara göre katılımcıların görevlerine göre bilgi güvenliği değişkenlerine verdikleri yanıtlar arasında anlamlı farklılık tespit edilememiştir. Bu doğrultuda H_{11} reddedilmiştir.

Tablo 16: Toplam İş Tecrübesine Göre Verilen Yanıtlar

	Toplam İş Tecrübesi	**N**	**Ortalama**	**Std. Sapma**	**T**	**p**
Bilgi Güvenliği Yaklaşımı	**10 yıdan az**	17	4,2721	,49457	2,151	,034
	10 yıldan fazla	85	3,9103	,65596		

Katılımcıların toplam iş tecrübelerine göre bilgi güvenliği değişkenlerine verdikleri yanıtlar arasında anlamlı bir farklılığın olup olmadığını tespit etmek amacıyla t testi gerçekleştirilmiştir. Tablo 16'da t testi sonucuna göre katılımcıların "Bilgi Güvenliği Yaklaşımı" değişkeni için anlamlı bir farklılık tespit edildiği görülmektedir. Bu doğrultuda "Bilgi Güvenliği Yaklaşımı" değişkeni için 10 yıldan az çalışanların verdikleri yanıtların ortalaması 4,27 ve 10 yıldan fazla süredir çalışanların verdikleri yanıtların ortalaması 3,91'dir. Bu doğrultuda, H_{12} "Bilgi Güvenliği Yaklaşımı" değişkeni için kabul edilmiştir.

Tablo 17: Katılımcıların İşyerine Çalışma Süresine Göre Verilen Yanıtlar

	İşyerinde Çalışma Süresi	N	Ortalama	Std. Sapma	T	P
Bilgi Güvenliği Yaklaşımı	5 yıl ve altı	29	4,1638	,76845	4,502	,013
	6-10 yıl arasında	29	4,0632	,67357		
	11 yıl ve üzeri	45	3,6778	,76616		
	Toplam	103	3,9231	,76711		

Katılımcıların iş yerlerinde çalışma sürelerine göre bilgi güvenliği değişkenlerine verdikleri yanıtlarda anlamlı bir farklılığın olup olmadığını tespit edebilmek amacıyla ANOVA testi gerçekleştirilmiştir. ANOVA testi sonucuna göre katılımcıların iş yerlerinde çalışma sürelerine göre "Bilgi Güvenliği Yaklaşımı" değişkenlerine verdikleri yanıtlarda anlamlı bir farklılık tespit edilmiştir. Bulgular Tablo 17'de ele alınmaktadır.

Bu doğrultuda "Bilgi Güvenliği Yaklaşımı" değişkeni için 5 yıl ve daha az süredir çalışan katılımcıların verdikleri yanıtların ortalaması 4,16, 6 ile 10 yıl arasında çalışan katılımcıların verdikleri yanıtların ortalaması 4,06 ve 11 yıl ve üzerinde süredir çalışan katılımcıların verdikleri yanıtların ortalaması 3,67'dir. Bu doğrultuda, H_{13} "Bilgi Güvenliği Yaklaşımı" değişkeni için kabul edilmiştir.

Hangi gruplar arasında farklılığın olduğunu tespit etmek amacıyla yapılan Post Hoc Testlerinden LSD analizi Tablo 18'de gösterilmektedir. Bu analize göre "Bilgi Güvenliği Yaklaşımı" değişkeni için 11 yıl ve daha fazla çalışan katılımcıların verdikleri yanıtlar ile 5 yıl ve altında süredir çalışan katılımcıların verdikleri yanıtlar (p=0,007) ve 6 ile 10 yıl arasında çalışan katılımcıların verdikler yanıtlar (p=0,032) arasında anlamlı bir farklılığın olduğu gözlenmektedir.

Tablo 18: Katılımcıların İş Yerlerindeki Çalışma Sürelerine İlişkin LSD Testi

LSD				
	(I)	(J)	Ortalama Farkları (I-J)	**p**
Bilgi Güvenliği Yaklaşımı	5 yıl ve altı	6-10 yıl arasında	,10057	,607
		11 yıl ve üzeri	,48602	**,007**
	6-10 yıl arasında	5 yıl ve altı	-,10057	,607
		11 yıl ve üzeri	,38544	**,032**
	11 yıl ve üzeri	5 yıl ve altı	-,48602	**,007**
		6-10 yıl arasında	-,38544	**,032**

Tablo 19'da görüldüğü gibi "Bilgi Güvenliği Yönetimi" değişkeni ile "Bilgi Güvenliği Yaklaşımı" değişkeni arasında pozitif yönde güçlü kuvvette bir ilişki ($p<0,001$ ve $r= 0,667$) olduğu görülmektedir. "Bilgi Güvenliği Yönetimi" değişkeni ile "Bilgi Güvenliği Uygulaması" değişkeni arasında pozitif yönde orta kuvvette bir ilişki ($p<0,001$ ve $r= 0,334$) vardır. "Bilgi Güvenliği Yönetimi" değişkeni ile "Bilgi Güvenliği Kültürü" değişkeni arasında pozitif yönde güçlü kuvvette bir ilişki ($p<0,001$ ve $r= 0,636$) vardır. "Bilgi Güvenliği Yönetimi" değişkeni ile "Bilgi Güvenliğinde Gizlilik" değişkeni arasındaki ilişki anlamlı değildir.

"Bilgi Güvenliği Yaklaşımı" değişkeni ile "Bilgi Güvenliği Uygulaması" değişkeni arasında pozitif yönde güçlü kuvvette bir ilişki ($p<0,001$ ve $r= 0,522$) vardır. "Bilgi Güvenliği Yaklaşımı" değişkeni ile "Bilgi Güvenliği Kültürü " değişkeni arasında pozitif yönde güçlü kuvvette bir ilişki ($p<0,001$ ve $r= 0,682$) vardır. "Bilgi Güvenliği Yaklaşımı" değişkeni ile "Bilgi Güvenliğinde Gizlilik" değişkeni arasındaki ilişki anlamlı değildir.

Tablo 19: Korelasyon Analizi (Bilgi Güvenliği)

		Bilgi Güvenliği Yönetimi	Bilgi Güvenliği Yaklaşımı	Bilgi Güvenliği Uygulaması	Bilgi Güvenliği Kültürü	Bilgi Güvenliğinde Gizlilik
Bilgi Güvenliği Yönetimi	R	1				
	Sig.					
	N	104				
Bilgi Güvenliği Yaklaşımı	R	,667	1			
	Sig.	,000				
	N	104	104			
Bilgi Güvenliği Uygulaması	R	,334	,522	1		
	Sig.	,001	,000			
	N	104	104	104		
Bilgi Güvenliği Kültürü	R	,636	,682	,497	1	
	Sig.	,000	,000	,000		
	N	103	103	103	103	
Bilgi Güvenliğinde Gizlilik	R	,132	,225	,010	,192	1
	Sig.	,181	,022	,917	,052	
	N	104	104	104	103	104

"Bilgi Güvenliği Uygulaması" değişkeni ile "Bilgi Güvenliği Kültürü " değişkeni arasında pozitif yönde orta kuvvette bir ilişki ($p<0,001$ ve $r= 0,497$) vardır. "Bilgi Güvenliği Uygulaması" değişkeni ile "Bilgi Güvenliğinde Gizlilik" değişkeni arasındaki ilişki anlamlı değildir. Son olarak, "Bilgi Güvenliği Kültürü" değişkeni ile "Bilgi Güvenliğinde Gizlilik" değişkeni arasındaki ilişki anlamlı değildir. Bu doğrultuda H_{14} "Bilgi Güvenliğinde Gizlilik" ve diğer değişkenler arasındaki ilişki dışında kabul edilmiştir.

- **Örgüt İklimi ve Bilgi Güvenliği İlişkisi**

Tablo 20: Korelasyon Analizi (Örgüt İklimi ve Bilgi Güvenliği)

		Örgüt İklimi	Bilgi Güvenliği
Örgüt İklimi	r	1	
	Sig.		
	N	106	
Bilgi Güvenliği	r	,509**	1
	Sig.	,000	
	N	104	104

Araştırma değişkenleri olan örgüt iklimi ve bilgi güvenliği arasındaki ilişkinin yönünü ve kuvvetini belirleyebilmek amacıyla korelasyon analizi gerçekleştirilmiştir. Bu doğrultuda "Örgüt İklimi" değişkeni ile "Bilgi Güvenliği " değişkeni arasında pozitif yönde güçlü kuvvette bir ilişki ($p<0,001$ ve $r= 0,509$) vardır. Elde edilen bulgular doğrultusunda H_{15} kabul edilmiştir.

- **Örgüt İklimi ve Bilgi Güvenliği İlişkisi**

Tablo 21'de "Bilgi Güvenliği Yönetimi" bağımsız değişkenleri ile "Örgüt İklimi Yaklaşımı" bağımsız değişkenleri arasındaki ilişkinin anlamlılığı gücü ve yönüne ilişkin bulgular yer almaktadır. "Bilgi Güvenliği Yönetimi" değişkeni ile "Organizasyon Yapısı" değişkeni arasında pozitif yönde orta kuvvette bir ilişki ($p<0,001$ ve $r= 0,369$) olduğu görülmektedir. "Bilgi Güvenliği Yönetimi" değişkeni ile "Bireysel Sorumluluk" değişkeni arasında pozitif yönde orta kuvvette bir ilişki ($p<0,001$ ve $r= 0,544$) vardır. "Bilgi Güvenliği Yönetimi" değişkeni ile "Ödüllendirme " değişkeni arasında pozitif yönde orta kuvvette bir ilişki ($p<0,001$ ve $r= 0,427$) vardır. "Bilgi Güvenliği Yönetimi" değişkeni ile "Risk Alma" değişkeni arasında pozitif yönde orta kuvvette bir ilişki tespit edilmiştir ($p<0,001$ ve $r= 0,485$). "Bilgi Güvenliği Yönetimi" değişkeni ile "Ilımlı Çalışma Ortamı" değişkeni arasında pozitif yönde orta kuvvette bir ilişki tespit edilmiştir ($p<0,001$ ve $r= 0,485$). Son olarak, "Bilgi Güvenliği Yönetimi" değişkeni ile "Destek" değişkeni arasında pozitif yönde orta kuvvette bir ilişki tespit edilmiştir ($p<0,001$ ve $r= 0,400$).

Tablo 21: Korelasyon Analizi (Örgüt İklimi Boyutları ve Bilgi Güvenliği Boyutları)

		Organizasyon Yapısı	Bireysel Sorumluluk	Ödüllendirme	Risk Alma	Ilımlı Çalışma Ortamı	Destek
Bilgi Güvenliği Yönetimi	r	,369	,544	,427	,485	,485	,400
	Sig.	,000	,000	,000	,000	,000	,000
	N	104	104	104	104	104	104
Bilgi Güvenliği Yaklaşımı	r	,323	,401	,373	,308	,308	,369
	Sig.	,001	,000	,000	,001	,001	,000
	N	104	104	104	104	104	104
Bilgi Güvenliği Uygulaması	r	,218	,293	,250	,282	,282	,220
	Sig.	,026	,003	,010	,004	,004	,025
	N	104	104	104	104	104	104
Bilgi Güvenliği Kültürü	r	,272	,389	,349	,398	,398	,354
	Sig.	,005	,000	,000	,000	,000	,000
	N	103	103	103	103	103	103
Bilgi Güvenliğinde Gizlilik	r	,075	,191	-,069	,125	,125	,060
	Sig.	,450	,052	,488	,205	,205	,545
	N	104	104	104	104	104	104

"Bilgi Güvenliği Yaklaşımı" değişkeni ile "Organizasyon Yapısı" değişkeni arasında pozitif yönde orta kuvvette bir ilişki ($p<0,001$ ve $r= 0,323$) olduğu görülmektedir. "Bilgi Güvenliği Yaklaşımı" değişkeni ile "Bireysel Sorumluluk" değişkeni arasında pozitif yönde orta kuvvette bir ilişki ($p<0,001$ ve $r= 0,401$) vardır. "Bilgi Güvenliği Yaklaşımı" değişkeni ile "Ödüllendirme " değişkeni arasında pozitif yönde orta kuvvette bir ilişki ($p<0,001$ ve $r= 0,373$)

vardır. “Bilgi Güvenliği Yaklaşımı” değişkeni ile “Risk Alma” değişkeni arasında pozitif yönde orta kuvvette bir ilişki tespit edilmiştir (p<0,001 ve r= 0,308). “Bilgi Güvenliği Yaklaşımı” değişkeni ile “Ilımlı Çalışma Ortamı” değişkeni arasında pozitif yönde orta kuvvette bir ilişki tespit edilmiştir (p<0,001 ve r= 0,308). Son olarak, “Bilgi Güvenliği Yaklaşımı” değişkeni ile “Destek” değişkeni arasında pozitif yönde orta kuvvette bir ilişki tespit edilmiştir (p<0,001 ve r= 0,369).

“Bilgi Güvenliği Uygulaması” değişkeni ile “Organizasyon Yapısı” değişkeni arasında pozitif yönde zayıf kuvvette bir ilişki (p<0,001 ve r= 0,218) olduğu görülmektedir. “Bilgi Güvenliği Uygulaması” değişkeni ile “Bireysel Sorumluluk” değişkeni arasında pozitif yönde zayıf kuvvette bir ilişki (p<0,001 ve r= 0,293) vardır. “Bilgi Güvenliği Uygulaması” değişkeni ile “Ödüllendirme ” değişkeni arasında pozitif yönde zayıf kuvvette bir ilişki (p<0,001 ve r= 0,250) vardır. “Bilgi Güvenliği Uygulaması” değişkeni ile “Risk Alma” değişkeni arasında pozitif yönde zayıf kuvvette bir ilişki tespit edilmiştir (p<0,001 ve r= 0,282). “Bilgi Güvenliği Uygulaması” değişkeni ile “Ilımlı Çalışma Ortamı” değişkeni arasında pozitif yönde zayıf kuvvette bir ilişki tespit edilmiştir (p<0,001 ve r= 0,282). Son olarak, “Bilgi Güvenliği Uygulaması” değişkeni ile “Destek” değişkeni arasında pozitif yönde zayıf kuvvette bir ilişki tespit edilmiştir (p<0,001 ve r= 0,220).

“Bilgi Güvenliği Kültürü” değişkeni ile “Organizasyon Yapısı” değişkeni arasında pozitif yönde zayıf kuvvette bir ilişki (p<0,001 ve r= 0,272) olduğu görülmektedir. “Bilgi Güvenliği Kültürü” değişkeni ile “Bilgi Güvenliği Uygulaması” değişkeni arasında pozitif yönde orta kuvvette bir ilişki (p<0,001 ve r= 0,389) vardır. “Bilgi Güvenliği Kültürü” değişkeni ile “Ödüllendirme ” değişkeni arasında pozitif yönde orta kuvvette bir ilişki (p<0,001 ve r= 0,349) vardır. “Bilgi Güvenliği Kültürü” değişkeni ile “Risk Alma” değişkeni arasında pozitif yönde orta kuvvette bir ilişki tespit edilmiştir (p<0,001 ve r= 0,398). “Bilgi Güvenliği Kültürü” değişkeni ile “Ilımlı Çalışma Ortamı” değişkeni arasında pozitif yönde orta kuvvette bir ilişki tespit edilmiştir (p<0,001 ve r= 0,398). “Bilgi Güvenliği Kültürü” değişkeni ile “Destek” değişkeni arasında pozitif yönde orta kuvvette bir ilişki tespit edilmiştir (p<0,001 ve r= 0,354). Son olarak, “Bilgi Güvenliğinde Gizlilik” değişkeni ile örgüt iklimi bağımsız değişkenleri arasında anlamlı farklılık tespit edilmemiştir.

- **Örgüt İklimine Bilgi Güvenliği Faktörlerinin Etkisi**

Örgüt iklimine bilgi güvenliği faktörlerinin etkisini belirleyebilmek amacıyla regresyon analizi gerçekleştirilmiştir. Bu doğrultuda, Tablo 22'de regresyon analizi gösterilmektedir.

Tablo 22: Örgüt İklimine Bilgi Güvenliği Faktörlerinin Etkisi

DEĞİŞKENLER	***B***	***T***	***Sig T***
Bilgi Güvenliği Yönetimi	,561	6,815	,000
SABİT	1,393	4,756	,000
Not: Multiple R: ,561; R Square: ,315; Adj. R Square: ,308; F: 46,450; Signif F< 0,001			

Tablo 22'de incelendiğinde F değerinin 46,450 ve Signif F değerinin <0,001 düzeyinde gerçekleştiği görülmektedir. Buna bağlı olarak Multiple R= ,561 ve Adjusted R Square= ,308 olarak gerçekleşmiştir. Regresyon analizinde elde edilen bu sonuçlara göre, "Örgüt İklimi"ni etkileyen bilgi yönetimi değişkeni "Bilgi Güvenliği Yönetimi" ($p<0,001$ ve $\beta= ,561$) olarak belirlenmiştir. Bu değişkenler örgüt iklimi ile ilgili çalışanların görüşlerini %32 oranında açıklamaktadır ($R^2=,315$).

5. TARTIŞMA

Günümüzde kuruluşların sahip olduğu en önemli sermaye bilgidir. Bilginin var olması onun kullanımını etkili kılmaz. Bilgiden istenilen düzeyde yarar sağlamak için, bilginin bir yönetim süreci olarak değerlendirilmesi ve ele alınması gerekir. Bilginin örgüt içi kullanımında, bilgiden beklenen fayda ve hedef belirlenmelidir. Bu nedenle örgüt için bilginin ortak amaç ve stratejileri belirlenmelidir. Bu süreçte bilginin örgüt için önemi ve getirisinin ne olduğu ve bilginin daha etkili ve verimli kullanımı için hangi faktörlerin önemli olduğu da belirlenmiş olur.

Bilgi güvenliği, bilginin gizliliği, bilginin bütünlüğü ve bilginin erişilebilirliğine gelebilecek zararlardan korunulmasıdır. Günümüz bilgi ve bilişim teknolojileri ilişkisi düşünüldüğünde, bilgi güvenliğinin sağlanmasının, bilişim teknolojilerinin güvenliği ile yakından ilgili olduğu anlaşılmaktadır. Bilişim teknolojileri güvenliği içerisine, donanım, yazılım, bilgi ve iletişimi kapsayan bilgi sistemlerinin gizlilik, güvenlik, bütünlük ve her zaman çalışır vaziyette olmasının sağlanması girmektedir (Onwubiko & Lenaghan, 2007).

Teknolojinin gelişmesi ile birlikte özel hayatın korunması konusu daha da önemli hale gelmiştir. Çünkü modern teknolojinin getirdiği araçlar insan yaşamının en önemli unsuru haline gelmiş ve bu araçlar ile kişilere ilişkin verilerin, bilgilerin hem elde edilmesi hem de yayılması oldukça kolaylaşmıştır. Kamu kurum ve kuruluşları, kendilerine ait işlevleri yerine getirirken vatandaşlara ait veri, bilgi ve işlemleri arşiv kayıtları arasına alıp vatandaşların işlemlerinin yapılmasında da bunlardan yararlanmaktadırlar. Kâğıtlar ve defterler üzerine işlenerek dosyalarda saklanan bu veriler, artık günümüzde bilgisayarlarda, elektronik ortamlarda tutulmaya ve ağlar üzerinden çok daha kolay bir şekilde paylaşılmaya başlanmıştır. Kâğıt ve defterlere işlenerek dosyalarda saklanan bilgilerin dahi ilgili kişinin özel hayatına zarar vermeyecek şekilde belirli kurallar altında yetkili kişiler tarafından bilinmesi, bunun dışında ki amaçlarla kullanılmaması sağlanmaya çalışılmıştır. Çünkü özel hayatın gizliliği öteden beri önemli bir insan hakkı olarak kabul edilmektedir. Elektronik ortamda bilgilerin elde edilmesinin ve yayılmasının daha kolay olduğu göz önünde bulundurulduğunda bu ortamlarda depolanan kişilere ait özel bilgilerin amacı dışında kullanılması ve/veya yayılması konusunun daha çok önem arz ettiği inkâr edilemez.

Bilişim teknolojilerinin sağladığı fayda ve olanaklar nedeniyle günümüzde çoğu işletme, faaliyetlerini gerçekleştirmek için bilişim teknolojilerine bağımlı hale gelmiştir. İşletmelerin

bilişim teknolojilerine bağlılığı arttıkça bu teknolojilerde meydana gelebilecek arızalara ve saldırılara karşı duyarlılığı da artmaktadır. İşletmenin bilgi işlem sistemine yapılacak bir saldırı ciddi miktarda para, zaman, itibar ve değerli bilgi kaybına sebep olabilmektedir (Dayıoğlu, 2002).

İşletmelerin birbirlerine elektronik ağlarla bağlandığı günümüzde güvenlik kaygısı zirvededir. 2007 CSI (Computer Crime & Security Survey) bilgisayar suçları ve güvenlik araştırmasına katılan işletmelerin en fazla karşılaştığı güvenlik ihlali sorununun işletme çalışanlarının suistimali (Katılanların %59'u) olduğu saptanmıştır. Bu oran, 2008 yılında %44 olarak saptanmıştır (2008, CSI). Oran düşmüş olsa bile yine de yüksek sayılabilecek bir düzeydedir. İşletmeler bilgi güvenliği konusunda kendi çalışanları sebebiyle önemli bir risk altında bulunmaktadır. Chang & Lin (2007)'ye göre çoğu bilgi güvenliği sorununun kaynağını dışarıdan bir saldırı değil insanların ihmalkârlığı oluşturmaktadır.

İşletmelerin sahip oldukları sınırlı kaynakları da bilgi güvenliğinin sağlanmasında bir kısıt oluşturmaktadır. İşletmelerin bilgi güvenliği harcamaları, işletmeden işletmeye ve sektörden sektöre değişmektedir. Karşılaşılabilecek güvenlik tehditlerinin çokluğuna karşın, işletmelerin güvenlik harcamaları sınırlıdır. Ayrıca, güvenlik uzmanları için "Ne kadar güvenlik yeterli?" cevaplaması zor bir sorudur (Johnson & Goetz, 2007).

Yapılan araştırmalar, yöneticilerin bilgi yönetimi konusuna gereken önemi verdiklerini göstermektedir. Stewart, işletmenin bilgi donanımına gerekli ve gerektiği kadar yatırım yaptıkları, bu donanımı kullanacak şekilde iş görenlerin eğitilmeleri veya eğitimli olanların işbaşına getirilmeleri konusuna ağırlık verdikleri, sürdürülebilir rekabet avantajı yakalamanın bilgi temelli yapılanmayı gerektirdiğini kabul etmektedirler (Demirel, 2008).

Örgütsel yapı bilgi yönetim süreçlerinin daha etkin çalışması için gereklidir ve örgütsel yapının bilgi yönetimi süreçlerinin aksamadan yürütülmesini sağlayacak şekilde tasarlanmış olması örgütsel etkinliği artıracaktır. Bu açıdan bakıldığında, örgüt içinde bilgi üretimini destekleyecek, elde edilen bu bilgiyi örgüte kolay aktarılabilecek bir şekilde tasarlayacak ve bu bilgiyi örgütte kullanmayı ve korumayı sağlayacak örgütsel yapılar oluşturmak, bilgi yönetimi sürecinin etkinliğini artıracaktır. Diğer bir ifade ile örgütsel yapının bürokratik olmayan bir şekilde ve açık iletişime olanak verecek bir biçimde tasarımı ile bilgi yönetiminin süreçlerini olumlu biçimde etkilemek mümkün olabilir. İşletmelerde oluşan kültürel ortam ve örgüt yapısı doğrudan örgütsel etkinliği artırabilmektedir. Çalışmada "Bilgi Güvenliği" değişkenleri ile

"Organizasyon Yapısı" değişkeni arasında pozitif yönde ($p<0,001$) olduğu görülmektedir. Örgütsel yapıyla, etkinlik arasındaki pozitif ilişkinin varlığı da Çakar'ın (2010) yaptığı araştırmanın sonuçlarıyla uyumlu görülmektedir.

Çalışmada örgüt iklimi değişkenlerinden ortaya çıkan en güçlü faktör (3.5±0,81) puan ortalaması ile "Risk Alma" ve "Ilımlı Çalışma Ortamı" olarak ortaya çıkmıştır. Özdere'nin (2010), yaptığı çalışmada "Yapısal Bağlılık" olarak konmuştur.

Çalışmada, demografik veriler incelendiğinde ankete katılanların çoğunluğunun cinsiyetinin kadın, yaş grubunun 41-50 yaş arası, lisans mezunu, başhermşire ve başhemşire yardımcılarının, toplam iş tecrübesinde 10 yıldan fazla olanların, işyerinde 11 yıl ve üzeri çalışanlar katılmıştır. Tecrübeli ve eğitimli çalışanların ankete katılması, çalışanların algılarını yansıtması açısından önemlidir.

Çalışmaya katılan katılımcılarda kadınların Örgüt ilkimi boyutlarından "Ödüllendirme" puan ortalaması bakıldığında (3.14±0,53) ve "Destek" puan ortalaması bakıldığında (3.5.±0,65) puan ortalaması olduğu görülmektedir. Başhemşire/ Başhemşire Yardımcılarının Örgüt ilkimi boyutlarından "Ödüllendirme" puan ortalaması bakıldığında (3.2±0,53) ve "Destek" puan ortalaması bakıldığında (3.6.±0,69) puan ortalaması olduğu görülmektedir. Analize göre "Ödüllendirme" değişkeni için başhemşire veya başhemşire yardımcılarının verdikleri yanıtlar ile müdür veya müdür yardımcılarının verdikleri yanıtlar arasında anlamlı bir farklılığın olduğu gözlenmektedir ($p<0,001$). "Destek" değişkeni için başhemşire veya başhemşire yardımcılarının verdikleri yanıtlar ile müdür veya müdür yardımcılarının verdikleri yanıtlar arasında anlamlı bir farklılığın olduğu gözlenmektedir ($p=0,006$). Sonuçlar göstermektedir ki, örgüt genelinde yeni uygulamalar düşünüldüğünde öncelikle örgütün iklimine bakmak gerekir. Zeffane'ye (1994) göre, çalışanların örgüte bağlılığı, heyecanı, morali, sadakati ve ilişkisi ile ilgili sorular yanıtlanırken yöneticilerin sadece motivasyon araç ve yöntemlerine bakmaları yetmez. Bu sorunlarla uğraşmak için yöneticiler aynı zamanda örgütte motivasyonu düşürücü etken ve olgulara uygulamalara da bakmak zorundadırlar. Yani örgüt iklimini daha iyi anlayabilmek için örgütsel destek çalışanlara sunulmalıdır. Örgütsel desteği sağlamadan örgüt ikliminin çağdaş yönetim uygulamalarındaki etkisi görülmeyebilir.

Bilgi güvenliği değişkenlerinden "Bilgi Güvenliğinde Gizlilik" puan ortalaması bakıldığında (4.2.±0,72) en yüksek ortalamaya ve "Bilgi Güvenliği Uygulaması" puan ortalaması bakıldığında (3.4.±0,82) ise en düşük ortalamaya sahiptir. Ekici (2007), ülkemizde kurulan Bilgi

Sistemleri (BS)'nin gecikmesine neden olan temel faktörler; BS yöneticilerinin olmaması, birim yöneticilerinin bilgi sistemlerini kabullenememesi, donanım ve yazılımların zamanında sağlanmaması, görev tanımlarının yapılmaması, organizasyonel yapıda BS'ye uygun yapılandırmaya gidilememesi olarak ortaya koymuştur.

İş yerinde lisans ve üzerinde eğitim düzeyine sahip katılımcıların bilgi güvenliği değişkenlerinden "Bilgi Güvenliğinde Gizlilik" değişkenine verdikleri yanıtların ortalaması (4.5.±0,57) dir. Bilgi güvenliği önemi önlisans eğitimine sahip olan personelde farkllılk olduğu görülüyor. Eğitim seviyesi arttıkça bilgi güvenliğinde gizlilikte artmaktadır.

Toplam iş tecrübelerinde 10 yıldan az çalışan katılımcıların bilgi güvenliği değişkenlerinden"Bilgi Güvenliği Yaklaşımı" değişkenine verdikleri yanıtların ortalaması (4.27.±0,49) dir. İş yerlerinde çalışma sürelerine göre 5 yıl ve daha az çalışan katılımcıların bilgi güvenliği değişkenlerinden "Bilgi Güvenliği Yaklaşımı" değişkenine verdikleri yanıtların ortalaması (4.16.±0,76) dir. Çalışma yılı artıkça çalışanlar tarafından bilgi güvenliğinin farkına varılması artmakta olduğu görülmektedir.

Elde edilen bulgulara göre, Bilgi güvenliği değişkenleri arasında anlamlı pozitif bir ilişki vardır ($p<0,001$). Örgüt iklimi değişkenleri arasında da anlamlı pozitif bir ilişki vardır ($p<0,001$). "Örgüt İklimi" değişkeni ile "Bilgi Güvenliği " değişkeni arasında pozitif yönde güçlü kuvvette bir ilişki" ($p<0,001$ ve $r= 0,509$) vardır. "Örgüt İklimi"ni etkileyen bilgi yönetimi değişkeni "Bilgi Güvenliği Yönetimi" ($p<0,001$ ve $\beta= ,561$) olarak belirlenmiştir. Bu değişkenler örgüt iklimi ile ilgili çalışanların görüşlerini %32 oranında açıklamaktadır ($R^2=,315$).

Yapılmış olan bu çalışmada, Sağlık kuruluşlarında örgüt iklimi ve bilgi güvenliği ilişkisi İzmir merkezde izin alınabilen hastanelerde incelenmiştir. Çalışmanın İzmir merkezle sınırlı oluşu ve yöneticilerle yapılmasından dolayı az sayıda anket elde edilmiştir. Gelecekteki çalışmalarda daha geniş bir alanda ve daha çok katılımcı ile çalışılması önerilmektedir.

6. SONUÇ VE ÖNERİLER

Bu çalışmanın amacı; son zamanlarda güncel olan bilgi güvenliğinin sağlık sektöründe örgüt iklimi ilişkisini ortaya çıkarmak, sağlık sektöründe örgüt ikliminin önemini vurgulamak, bilgi güvenliğinin örgüt iklimindeki yerini belirlemektir. Bu çalışmada bilgi güvenliği oluşumunda örgüt iklimi ne kadar önemli bir etkiye sahip olduğu belirtmek ve ölçmektir.

Araştırmanın bulgularına göre yöneticilere ve araştırmacılara aşağıdaki önerilerde bulunulmuştur.

- Çalışan ve yöneticilerin bilgi yönetimine yönelik beceri ve yeteneklerinin geliştirilmesi etkili bir eğitim süreciyle sağlanabilir. Bilginin yönetimi, kendilerini geliştirmiş birey ve yöneticilerin önderliğinde tam katılımla örgüt içinde rasyonel bir şekilde uygulanabilir.
- Örgüt öncelikle bilgi yönetimi süreçlerinin sağlıklı ilerleyebilmesi için örgüt yapısını bu sisteme göre tasarlamalı ve örgüt ikliminin bilgi yönetimini özümseyecek bir düzeyde oluşturmalıdır. Örgüt yapısı ve örgüt iklimi güçlü olduğu takdirde örgüt bilgiyi etkin şekilde elde edebilir.
- Bilgi yönetimine odaklı örgütsel bir yapının oluşturulmasında ödüllendirme ve destek önemlidir.
- Bilgi güvenliği yönetiminde yöneticiler kararlı olmalıdırlar. Bilgi güvenliğinin etkin bir şekilde saklanması, alınacak teknik önlemlerin yanında işletmenin sahip olduğu bilgi güvenliği kültürüne de bağlıdır.

7. KAYNAKLAR

Acılar A. İşletmelerde Bilgi Güvenliği ve Örgüt Kültürü Organizasyon. Yönetim Bilimleri Dergisi, 2009; 1:25-33.

Alkan N. Tıp ve Sağlık Kuruluşlarında Bilgi Yönetimi, ÜNAK'03: Bilgiye Erişimde Değişen Yollar ve II. Tıbbi Bilgi Yönetimi ve Teknolojileri Sempozyumu,2003; 176-186. http://kaynak.unak.org.tr/bildiri/unak03/u03-21.pdf

Al-Shammari MM. Organizational Climate, Leadership&Organization Development Journal, 1992 ;13: 30-32.

Arslan NT. Örgütsel Performansı Belirleyici Bir Etmen Olarak Örgüt Kültürü ve İlimi Hakkında Bir Değerlendirme. Isparta, Süleyman Demirel Üniversitesi, İ.İ.B.F. Dergisi, 2004;9: 203–228.

Audrey SB, Smith R D. Managing Organizational Knowledge As A Strategic Asset .Journal Of Knowledge Management, 2001; 1.

Aydınlı C. ISO 27001 Bilgi Güvenliği Yönetim Sistemi Standardı. SABİYAP, 2009:3:16-20.

Aytaç S. Çalışma Psikolojisi Alanında Yeni Bir Yaklaşım: Örgütsel Sağlık. İş, Güç, Endüstri İlişkileri ve İnsan Kaynakları Dergisi, 2003;5.

Barman S. Writing Information Security Policies, New Riders Publishing, 2001.

Barutçugil İ.Bilgi Yönetimi, İstanbul, Kariyer Developer Yayınları, 2002.

Batlis N.The Effects Of Organizational Climate On Job Satisfaction, Anxiety And Propensity To Leave, The Journal Of Psychology, 1980; 104: 233-240.

Bucak EB. Abant İzzet Baysal Üniversitesi Eğitim Fakültesinde Örgüt İklimi: Yönetimde Ast-Üst İlişkileri. Muğla Üniversitesi, SBE Dergisi Bahar Sayı, 2002;7.

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

Celep C, Çetin B. Bilgi Yönetimi, Ankara, Anı Yayıncılık, Ankara, 2003, 10–12.
Çetin A, Aydos M. Elektronik Sağlık Kayıtları Güvenliğinde IEEE 802.1x Standardının Kullanılması. 2006:1-5. http://www.iscturkey.org/2010/2008/2006/pdf/bildiri/11.pdf

Çetin MÖ. Örgüt Kültürü ve Örgütsel Bağlılık, Ankara, Nobel Yayın Dağıtım, 2004.

Cura T. Yöneticiler İçin Bilişim Teknolojileri ve Enformasyon Sistemleri, İstanbul, Sistem Yayıncılık, 2009.

Çapar B. Bilgi Yönetimi: Nasıl Bir İnsan Gücü?. II. Ulusal Bilgi, Ekonomi ve Yönetim Kongresi Bildirileri: 421-432, 2003, İstanbul.

Davenport T, Prusak L. İş Dünyasında Bilgi Yönetimi, İstanbul, Rota Yayınları, 2001.

Dayıoğlu B. Ağ ve İşletim Sistemi Güvenliği. Türkiye Bilişim Derneği 9. Bilgi İşlem Merkezi Yöneticileri Semineri: 2002:108-114, Antalya.

Demirel Y, Seçkin Z. Bilgi Yönetimi Uygulamasında Etkili Olan Faktörler Üzerine Mobilyacılık Sektöründe Bir Araştırma. ZKÜ Sosyal Bilimler Dergisi, 2008:107:122.

Dervişoğlu HG. Stratejik Bilgi Yönetimi, İstanbul, Dışbank Kitapları, 2004.

Dıxon N.The Organizational Learning Cycle: How We Can Learn Collectively, London, McGraw Hill Book Company, 1994.

Doğantimur F.ISO 27001 Standardı Çerçevesinde Kurumsal Bilgi Güvenliği, Mesleki yeterlilik tezi, Maliye bakanlığı Strateji Geliştirme Başkanlığı, 2009:7-10.

DPT Bilgi Toplumu Dairesi.E-Dönüşüm Türkiye Projesi Birlikte Çalışabilirlik Esasları Rehberi Sürüm 2.0,2009.
http://www.bilgitoplumu.gov.tr/Documents/1/Yayinlar/090228_BirlikteCalisabilirlikEsaslariv2.pdf

Flint N. Culture Club: An Investigation of Organizational Culture, Sydney, Aare, 2000.

Gayef A. Özel Hastanelerde Uygulanan Liderlik Yaklaşımlarının Üst Düzey Yöneticilerin Takım Çalışması ve Örgüt İklimi Algılamaları Üzerindeki Etkisi, İstanbul Üniversitesi, Sosyal Bilimler Enstitüsü, Hastane ve Sağlık Kuruluşlarında Yönetim Bilim Dalı Yüksek Lisans Tezi, 2006.

Gold H.A, Malhotra A, Segars AH. Knowledge Management: An Organizational Capabilities Perspective. Journal of Management Information Systems, 2001;18: 185-214.

Gürkan GÇ. Örgütsel Bağlılık: Örgütsel İklimin Örgütsel Bağlılık Üzerindeki Etkisi ve Trakya Üniversitesi'nde Örgüt İklimi İle Örgütsel Bağlılık Arasındaki İlişkinin Araştırılması, Edirne, Trakya Üniversitesi, Sosyal Bilimler Enstitüsü, 2006.

Güven M, Açıkgöz B.Yöneticilerin Örgüt Kültürü Algılamalarına İlişkin Bir Analiz: Zonguldak Karaelmas Üniversitesi Örneği. ZKÜ Sosyal Bilimler Dergisi, 2007; 3: 1–20.
https://www.callio.com/files/wp_iso_en.pdf

Halpin A. Theory and Research in Administration, New York ,The MacMillan Co, 1966,174-181.

Hocanizov N. Ağırlama İşlemelerinde Örgüt İklimi ve Liderlik, İzmir, Dokuz Eylül Üniversitesi Turizm İşletmeciliği Anabilimdalı Yüksek Lisans Tezi, 2008.

Hülür Ü. Bilgi Güvenliği ve Sağlık. SABİYAP, 2009:3:6-8.

Karahan A, Yılmaz, H. Öğrenen Örgüt ve Bilgi Yönetimi İlişkisi: Afyonkarahisar İlinde Bulunan Hastane Yöneticileri Üzerine Bir Araştırma. Eskişehir Osmangazi Üniversitesi İİBF Dergisi, 2010; 5: 147-174. http://iibf.ogu.edu.tr/dergi/dergi/2010-1/2010_1_8.pdf

Karcıoğlu F. Örgüt Kültürü ve Örgüt İklimi İlişkisi. İktisadi ve İdari Bilimler Dergisi, 2001; 15: 1-2.

Kovacıch GL. The Information Systems Security Officer's Guide: Establishing and Managing an Information Protection Program, Second Edition, Butterworth Heinemann, 2003.

Kumaş E. Kurumlarüstü Bilgi Güvenliği Stratejisi. Uluslararası Katılımlı Bilgi Güvenliği ve Kriptoloji Konferansı :330-335, 2007, Ankara.

Küçükgöde V. Çukurova Üniversitesi Ziraat Fakültesi Öğretim Üyelerinin Örgüt İklimi Hakkındaki Düşünceleri, Çukurova Üniversitesi Fen Bilimleri Enstitüsü Tarım Ekonomisi Anabilim Dalı, 2005.

Küçükoğlu Ş. Uygun Güvenlik Çözümüne Yolculuk, 2005.
http://www.infosecurenet.com/macroscope/macroscope6.pdf.(08/12/2010)

Lim HD, Morris LM. Influence of Traince Chracteristics, İnstructional Satisfaction and Organizational Climate on Percievet Learning and Training Transfer. Human Reseorce Development Quarterly, 2006;17(1):85–115.

Marsap A, Akalp G,Yeniman E. Sağlık İşletmelerinde İnsan Kaynağının Kurumsal Bilgi Güvenliği Kültürü Gelişimi. Bilişim Teknolojileri Dergisi, 2010; 3: 31-40.

Mullins LJ. Management and Organizational Behavior, (2nd Ed.), Great Britain, Pitmann Publishing, 1989.

Nonaka I. The knowledge creating company. Harvard Business Review On Knowledge Management, USA: Harvard Business School Pres,1998.

O'Dell C, Grayson J, Essaıdes N. (2003). Ne Bildiğimizi Bilseydik, İstanbul, Dışbank Yayınları, 2003.
Odabaş H. Bilgi Yönetimi Sistemi. Bilgi Çağı Bilgi Yönetimi ve Bilgi Sistemleri İçinde, Konya, Çizgi Kitabevi, 2005.

Onat A. Özel Hastanelerde Bilgi Yönetimi: Bir Araştırma, İstanbul Üniversitesi, Sosyal Bilimler Enstitüsü, Hastane ve Sağlık Kuruluşlarında Yönetim Bilim Dalı Yüksek lisans Tezi, 2010:3-9.

Saka O. Tıp Bilişiminde Neredeyiz?, Tıp Bilişimi Derneği Güz Okulu Seminer Notları, Antalya, 2004.

Özdemirci F, Aydın C. Kurumsal Bilgi Kaynakları ve Bilgi Yönetimi. Türk Kütüphaneciliği 22, 2008;1:59-81.

Özdemir F. Örgütsel İklimin İş Tatmin Düzeyine Etkisi: Tekstil Sektöründe Bir Araştırma, Adana, Çukurova Üniversitesi, Sosyal Bilimler Enstitüsü, İşletme Anabilim Dalı, 2006.

Özdere A. Bir Yükseköğretim Kurumunda, ISO 9001:2000 Kalite Yönetim Sistemi Belgesine Sahip Olan ve Olmayan Birimler Arasındaki Örgüt İklimi Farklılıkları: Dokuz Eylül Üniversitesi Örneği, İzmir, Dokuz Eylül Üniversitesi Sosyal Bilimler Enstitüsü Toplam Kalite Anabilimdalı, 2010.

Raymond MJ, George S. Management Information System. Upper Saddle River, Pearson Education, 2004.

Rodoplu D. Bilgi Teknolojileri Uygulamalarına Karşı Çalışan Direnci; Hastane Bilgi Sistemi Üzerinde Bir Uygulama. Review of Social, Economic & Business Studies, 2006:9: 409-438.

Schein EH. Örgütsel Kültür**.** Dokuz Eylül Üniversitesi SBE Dergisi, 2002;4:7.

Siu O. Predictors of job satisfaction and absenteeism in two samples of Hong Kong nurses. Journal of Advanced Nursing, 2002; 40:218-229.
Şişman M. Örgütler ve Kültürler, Ankara, Pegem Yayıncılık, 2002.

Şişman M, Turan S. Örgütsel Semboller ve Eğitimde Sembolik Liderlik. Kuram ve Uygulamada Eğitim Yönetimi Kış Sayı, 2004; 37: 96– 117.

Tarı B. Analyzing The Fit Between Organizational Environment, Structure and Culture: A Case Study Of A Bublic Organization. Ankara, Orta Doğu Teknik Üniversitesi, Sosyal Bilimler Enstitüsü, İşletme Anabilim Dalı, 2002.

Taşkın E, Sezici E, Oğuz A. Bilgiye Dayalı Yönetim. Dumlupınar Üniversitesi Sosyal Bilimler Enstitüsü Dergisi, 2001; 3: 5.

Tekerek M. Bilgi Güvenliği Yönetimi. KSÜ Fen Fakültesi Mühendislik Fakültesi Dergisi, 2008;11:132-137.

Terzi AR. Örgüt Kültürü, 1.Baskı, Ankara: Nobel Yayın Dağıtım, 2002.

Thow-Chang L, Siew-Mun K, Foo A. Information Security Management Systems and Standards. Synthesis Journal, 2001; 2:5-8.

Tiwana A. Bilginin Yönetimi, İstanbul, Dışbank Kitapları, 2003.

Türk Standartları Enstitüsü, "Bilgi Teknolojisi-Güvenlik Teknikleri-Bilgi Güvenliği Yönetim Sistemleri-Gereksinimler", TS ISO / IEC 27001:2005, Mart 2006.

TS ISO/IEC 13335-1. Guidelines For The Management Of IT Security Part 1: Concepts And Models For IT Security,2004.

TS ISO/IEC 27799 “Sağlık Bilişim - Sağlık Bilgi Güvenliği Yönetimi Kullanarak ISO/IEC 27002

TS ISO/IEC 17799- Bilgi Güvenliği Yönetimi için Uygulama Sistemleri.

Tonta, Y. Bilgi Yönetiminin Kavramsal Tanımı ve Uygulama Alanları, Kütüphaneciliğin Destanı Sempozyumu, 2004, Ankara.
http://www.yunus.Hacettepe.edu.tr/~tonta/yayinlar/bilgiyonetimi.ppt

Tuğlular T. Üniversitelerde Bilgi Güvenliği Politikaları, Ulaknet Sistem Yönetimi Konferansı – Güvenlik, 2003.
http://www.ulakbim.gov.tr/dokumanlar/guvenlik/Tugkan_Tuglular.pdf

Ulaşanoğlu ME, Yılmaz R, Tekin MA. Bilgi Güvenliği: Riskler ve Öneriler, Bilgi Teknolojileri ve İletişim Kurumu, 2010:7-10.

Vural Y, Sağıroğlu Ş. Kurumsal Bilgi Güvenliği ve Standartları Üzerine Bir İnceleme. Gazi Üniversitesi Müh. Fak. Dergisi, 2008;23:507-522.

Wilson TD. (2002). Information management. In International Encyclopedia of Information and Library Science. In. Feather J, Sturges P, editors. 2d London: Routledge http://informationr.net/tdw/publ/papers/encyclopedia_entry.html

Yeniçeri Ö, İnce M. Bilgi Yönetimi Stratejileri ve Girişimcilik. İstanbul, Kültür Sanat Yayınları, 2005.

Yıldız B. Bilgi Güvenliği ve E-Devlet Kapsamında Kamu Kurumlarında Bilgi Güvenliği Yönetim Standartlarının Uygulanması, Gebze Yüksek Teknoloji Enstitüsü Sosyal Bilimler Enstitüsü Yüksek lisans tezi, 2007.

Yılmaz M. Örgütsel Öğrenmede Bilgi Merkezinin Rolü, Ankara Üniversitesi Sosyal Bilimler Enstitüsü Yayınlanmamış Doktora Tezi Ankara, 2008.

Yozgat U. Yönetim Bilişim Sistemleri, İstanbul, Beta Basım Yayını,1998, 374-397.

EK-1: Etik Kurul Onayı

DOKUZ EYLÜL ÜNİVERSİTESİ
GİRİŞİMSEL OLMAYAN ARAŞTIRMALAR ETİK KURULU

Konu: Karar hk. /207 12.04.2011

Doç.Dr.Özlem İpekgil DOĞAN
Doç.Dr.Şeyda Seren İNTEPELER
Yük.Lis.Öğr.Başak GERÇEKER
DEU İktisadi ve İdari Bilimler Fakültesi, İşletme Bölümü

Kurulumuz tarafından 31.03.2011 tarih ve 144-GOA protokol numaralı 2011/10-07 karar numarası ile görüşülen **"Sağlık Kuruluşlarında Örgüt İklimi ve Bilgi Güvenliğinin İlişkisi"** konulu araştırmanıza ilişkin Kurulumuz kararı ekte sunulmuştur.

Bilgilerinizi ve gereğini rica ederim.

Prof.Dr.Banu ÖNVURAL
Başkan

Ek: Etik Kurul Kararı

Dokuz Eylül Üniversitesi Sağlık Yerleşkesi İnciraltı 35340 İZMİR-TÜRKİYE
Tel:0 232 4122254 - 0 232 4122258 Faks: 0232 4122243 Elektronik posta:etikkurul@deu.edu.tr

DOKUZ EYLÜL ÜNİVERSİTESİ
GİRİŞİMSEL OLMAYAN ARAŞTIRMALAR ETİK KURUL KARARI

ETİK KOMİSYONUN ADI	**DOKUZ EYLÜL ÜNİVERSİTESİ GİRİŞİMSEL OLMAYAN ARAŞTIRMALAR ETİK KURULU**
AÇIK ADRES	**Dokuz Eylül Üniversitesi Tıp Fakültesi Dekanlığı 2. Kat İnciraltı-İZMİR**
TELEFON	**0 232 412 22 54-0 232 412 22 58**
FAKS	**0 232 412 22 43**
E-POSTA	**etikkurul@deu.edu.tr**

BAŞVURU BİLGİLERİ	DOSYA NO:	144-GOA	
	ARAŞTIRMA	UZMANLIK TEZİ ☐	AKADEMİK AMAÇLI ☐
	ARAŞTIRMANIN AÇIK ADI	Sağlık Kuruluşlarında Örgüt İklimi ve Bilgi Güvenliğinin İlişkisi	
	ARAŞTIRMA PROTOKOL KODU	-	
	SORUMLU ARAŞTIRMACI ÜNVANI/ADI/SOYADI ve UZMANLIK ALANI	Doç.Dr.Özlem İpekgil DOĞAN Doç.Dr.Şeyda Seren İNTEPELER Yük.Lis.Öğr.Başak GERÇEKER DEU İktisadi ve İdari Bilimler Fakültesi, İşletme Bölümü	
	DESTEKLEYİCİ VE AÇIK ADRESİ	-	
	DESTEKLEYİCİNİN YASAL TEMSİLCİSİ VE ADRESİ	-	
	ARAŞTIRMAYA KATILAN MERKEZLER	TEK MERKEZ ☒	ÇOK MERKEZLİ☐

	Belge Adı	Tarihi	Versiyon Numarası	Dili
DEĞERLENDİRİLEN BELGELER	ARAŞTIRMA PROTOKOLÜ	Mevcut		Türkçe ☒ İngilizce ☐ Diğer ☐
	ARAŞTIRMA İLE İLGİLİ LİTERATÜR	Mevcut		Türkçe ☐ İngilizce ☒ Diğer ☐
	BİLGİLENDİRİLMİŞ GÖNÜLLÜ OLUR FORMU	Mevcut		Türkçe ☒ İngilizce ☐ Diğer ☐
	OLGU RAPOR FORMU	Mevcut		Türkçe ☒ İngilizce ☐ Diğer ☐

KARAR BİLGİLERİ	**Karar No:2011/10-07**	**Tarih:31.03.2011**
	Doç.Dr.Özlem İpekgil DOĞAN Doç.Dr.Şeyda Seren İNTEPELER sorumlusu Yük.Lis.Öğr.Başak GERÇEKER'in yürütücüsü olduğu "**Sağlık Kuruluşlarında Örgüt İklimi ve Bilgi Güvenliğinin İlişkisi**" isimli klinik araştırmaya ait başvuru dosyası ve ilgili belgeler araştırmanın gerekçe, amaç, yaklaşım ve yöntemleri dikkate alınarak incelenmiş, etik açıdan çalışmanın gerçekleştirilmesinin uygun olduğuna oy birliği ile karar verilmiştir.	

ETİK KURUL BİLGİLERİ	
ÇALIŞMA ESASI	Dokuz Eylül Üniversitesi Etik Kurullar Yönetmeliği , İyi Klinik Uygulamaları Kılavuzu

ETİK KURUL ÜYELERİ

Unvanı/Adı/Soyadı	Uzmanlık Alanı	Kurumu	Cinsiyet	Araştırma ile İlişkili mi?		İmza
Prof.Dr.Banu ÖNVURAL (Başkan)	Tıbbi Biyokimya	DEU Tıp Fakültesi Tıbbi Biyokimya Anabilim Dalı	Kadın	E ☐	H ☒	
Prof.Ph.D.Besti ÜSTÜN (Başkan Yardımcısı)	Ph.D.Yüksek Hemşire	DEU Hemşirelik Yüksekokulu	Kadın	E ☐	H ☒	
Prof.Dr.Osman AÇIKGÖZ	Fizyoloji	DEU Tıp Fakültesi Fizyoloji Anabilim Dalı	Erkek	E ☐	H ☒	
Prof.Dr.Mehtap MALKOÇ	Ph.D.Fizik Tedavi ve Rehabilitasyon	DEU Fizik Tedavi ve Rehabilitasyon Yüksekokulu	Kadın	E ☐	H ☒	
Prof.Ph.D.Zuhal BAHAR	Ph.D. Yüksek Hemşire, Halk Sağlığında doktora	DEU Hemşirelik Yüksekokulu	Kadın	E ☐	H ☒	
Prof.Dr.Nejat SARIOSMANOĞLU	Kalp Damar Cerrahisi	DEU Tıp Fakültesi Kalp Damar Cerrahisi Anabilim Dalı	Erkek	E ☐	H ☒	
Prof.Dr.Ömer Selahattin TOPALAK	İç Hastalıkları (Gastroenteroloji)	DEU Tıp Fakültesi İç Hastalıkları Anabilim Dalı	Erkek	E ☐	H ☒	
Prof.Dr.Ece BÖBER	Pediatrik Endokrinoloji	DEU Tıp Fakültesi Çocuk Sağlığı ve Hastalıkları Anabilim Dalı	Kadın	E ☐	H ☒	
Prof.Dr.Hüseyin BASKIN	Mikrobiyoloji	DEU Tıp Fakültesi Mikrobiyoloji Anabilim Dalı	Erkek	E ☐	H ☒	
Doç.Dr.Servet AKAR	İç Hastalıkları (Romatoloji)	DEU Tıp Fakültesi İç Hastalıkları Anabilim Dalı	Kadın	E ☐	H ☒	
Doç.Dr.Mukaddes GÜNELİ	Tıbbi Farmakoloji	DEU Tıp Fakültesi Tıbbi Farmakoloji Anabilim Dalı	Kadın	E ☐	H ☒	
Doç.Dr.Ayşe Aydan ÖZKÜTÜK	Mikrobiyoloji	DEU Tıp Fakültesi Mikrobiyoloji Anabilim Dalı	Kadın	E ☐	H ☒	
Doç.Dr.Işıl TEKMEN	Histoloji ve Embriyoloji	DEU Tıp Fakültesi Histoloji ve Embriyoloji Anabilim Dalı	Kadın	E ☐	H ☒	
Prof.PhD.Meltem Kutlu GÜRSEL	Hukuk	D.E.Ü Hukuk Fakültesi İdare Hukuku Anabilim Dalı	Kadın	E ☐	H ☒	
İhsan ÇELİKDEMİR	Sağlık mensubu olmayan üye	75. Yıl Özel İlköğretim Okulu Müdür Yrd.	Erkek	E ☐	H ☒	

EK-2 Özgeçmiş

ÖZGEÇMİŞ

TC Kimlik No / Pasaport No:	49792486852
Doğum Yılı:	1980
Yazışma Adresi:	Dokuz Eylül Üniversitesi Sağlık Bilimleri Enstitüsü İnciraltı/İZMİR.
Telefon:	0 505 3958240
Faks:	-
e-posta:	bskgrckr35@gmail.com

EĞİTİM BİLGİLERİ

Ülke	Üniversite	Fakülte/Enstitü	Öğrenim Alanı	Derece	Mezuniyet Yılı
TR	Dokuz Eylül Üniversitesi	Hemşirelik Fakültesi	HEMŞİRE	Lisans	2007

AKADEMİK/MESLEKTE DENEYİM

Kurum/Kuruluş	Ülke	Şehir	Bölüm/Birim	Görev Türü	Görev Dönemi
-	-	-	-	-	-

UZMANLIK ALANLARI

Uzmanlık Alanları
-

ÖDÜLLER

	Ödülün Adı	Alındığı Kuruluş	Yılı
☐	-	-	-

EK-3 ANKET

Sayın Katılımcı,

Bu çalışma Dokuz Eylül Üniversitesi Sağlık Bilimleri Enstitüsü Sağlıkta Kalite Geliştirme ve Akreditasyon Anabilim Dalında yüksek lisans programında yürütülen bir tez çalışmasıdır. "Sağlık Kuruluşlarına Örgüt İklimi İle Bilgi Güvenliğinin İlişkisi" ortaya koymaktır.Anketi doldurmak sadece beş dakikanızı alacaktır. Çalışmanın sonuçları bilimsel araştırma amaçlı kullanılacaktır ve elde edilen veriler gizli tutulacaktır. Katılımınız için teşekkür eder, saygılar sunarız.

Doç.Dr ÖZLEM DOĞAN
D.E.Ü İ.İ.B.F
İŞLETME BÖLÜMÜ

BAŞAK GERÇEKER
D.E.Ü SBE
Sağlıkta Kalite Geliştirme ve Akreditasyon Öğrencisi

ÖRGÜT İKLİMİ	Tamamen Katılıyorum	Katılıyorum	Ne Katılıyorum Ne Katılmıyorum	Katılmıyorum	Tamamen Katılmıyorum
ORGANİZASYON YAPISI					
1. Kurumuzda yapılan işler açıkça tanımlanmıştır.					
2.Karar alma sürecinde kimin özel otoriteye sahip olduğu bazen belirsizdir.					
3.Örgütün politikaları ve organizasyon yapısı açıkça tanımlanmıştır.					
4.Bürokrasi minimum seviyededir.					
5. Aşırı kurallar ve bürokrasi yeni fikirlerin dikkate alınmasını güçleştirmektedir.					
6.Kurumumuzun verimliliği planlama yetersizliğinden dolayı azalmaktadır.					
7. Bulunduğum bazı projelerde kimin yöneticim olduğunda emin olamıyorum.					
BİREYSEL SORUMLULUK					
8. Kurumumuzun problemlerden biri de bireylerin sorumluluk almamalarıdır.					
9. Çalışanların işle ilgili problemlerini çözebilecekleri felsefesi kabul edilir.					
10.Yönetim, çalışanlarına rehber oluşturacak ilkeleri belirler .					
11.Yönetim, çalışanların işlerinde sorumluluk almalarına imkan verir.					
ÖDÜLLENDİRME					
12.Çalışanların yükseltilmesine dayalı bir ödüllendirme sistemi vardır.					
13.Kişilerin aldığı ödül ve teşvikler, eleştiri ve tehditlerden daha fazladır.					
14.Çalışanlar iş performansları ölçüsünde ödüllendirilmektedirler.					
15.Büyük oranda bir eleştiri vardır.					
16.Yapılan iyi işlerin karşılığında yeterli derecede ödül verilmemektedir.					
17. Çalışanlar yanlış yaptıklarında cezalandırılmaktadırlar.					
RİSK ALMA					
18. Yönetim, iyi bir fikre deneme şansı verme yönünde isteklidir.					
19. Bu sektörde rekabet avantajını korumak için risk almak zorundayız.					
20. Maksimum etkililik için karar alma sürecine tedbirli yaklaşılır.					
21. İşimiz doğru zamanda hesaplanan riskleri göze alarak kurulmuştur.					
ILIMLI ÇALIŞMA ORTAMI					
22. Bu işletmede çalışanlar arasında arkadaşça bir atmosfer hakimdir.					
23. Bu işletme ılımlı ve sakin bir çalışma iklimi ile nitelendirilmektedir.					
24. Bu işletmedeki çalışanlar soğuk ve birbirine uzak durmaz.					
25 Bu işletmede çalışanlar ile yönetim arasında ılımlı bir ilişki vardır.					
DESTEK					
26.Üst yönetim, çalışanların hata yapması durumunda onlara destek olmaz.					
27. Yönetim çalışanların kariyer beklentileri ile ilgilenir.					
28. Çalışanlar arasında yeterince güvene dayalı bir ilişki sistemi yoktur.					
29. Yönetimin temel felsefesi insan faktörüne ve düşüncelerini önem vermektir					
30. Zor bir projede arkadaşlarımdan ve yönetimden destek göreceğime inanırım.					

BİLGİ GÜVENLİĞİ	Tamamen Katılıyorum	Katılıyorum	Ne Katılıyorum Ne Katılmıyorum	Katılmıyorum	Tamamen Katılmıyorum
GENEL SAĞLIK BİLGİ GÜVENLİĞİ					
1. Kurumuzda bilgi güvenliği hedefleri belirlenmiştir.					
2. Kurumsal bilgi güvenliği yönetim sistemi oluşturulmuştur.					
3. Sağlık bilgi güvenliğindeki tehditler ve güvenlik açıklıkları nettir.					
4. Korunacak sağlık bilgileri belirlenmiştir.					
5. Kurumsal bilgi güvenliği klinik bazında izlenmektedir.					
SAĞLIKTA GENEL BİLGİ GÜVENLİĞİ UYGULAMASI					
6.Kurumuzda bilgi güvenliği uygulamasında yönetim kararlıdır.					
7.Bilgi güvenliği komitesi bulunmaktadır.					
8.Sistematik risk yönetimi uygulaması bulunmaktadır.					
9.Yönetim kaynakları etkin bir şekilde kullanır.					
10. Benzer kurumlarla bilgi güvenliği kıyaslaması yapılmaktadır.					
11. Bilgi güvenliği iç denetimi yapılmaktadır.					
12. Bilgi güvenliği yönetim sistemi, ilerlemeyi sağlar.					
SAĞLIKTA DETAY BİLGİ GÜVENLİĞİ UYGULAMASI					
13. Kişisel sağlık bilgilerinin korunması gerekli değildir.					
14. Bilgi güvenliği politikası bulunmaktadır.					
15. Bilgi güvenliği sorumluları belirlidir.					
16. Kişisel sağlık verilerini korumak için kurallar bulunmaktadır.					
17. Tüm kişisel sağlık verileri gizli tutulmalıdır.					
18. Kendi sağlık bilgilerimin arkadaşlarım tarafından görülmesini isterim.					
19. Kurumdan ayrılan personelin kullanıcı erişim yetkileri hemen iptal edilir.					
20. Kurumumuzda fiziksel ve çevresel güvenlik sağlanmaktadır.					
21. Kişisel sağlık bilgileri şifreli bir formatta tutulmaktadır.					
22. Acil durumlarda erişim kontrol kuralları belirlidir.					
23. Bilgi sistemleri edinmenin kuralları bulunmaktadır.					
24.Bilgi güvenliği güvenlik olayları etkili bir şekilde sonuçlanır.					
25.Kurumumuzda bilgi güvenliği gereklilik olarak kabul edilmiştir.					
26. Bilgi güvenliği yönetim sistemi sağlıklı uygulanmaktadır.					

DEMOGRAFİK VERİLER

1. Cinsiyetiniz.
1.( )Kadın 2.( )Erkek
2. Yaşınız.
1.()20 den az 2.( )20-30 3.( )31-40 4.( ) 41-50 5.( )51 ve üzeri
4. Eğitim Durumunuz.
1.( )Lise 2.( )Ön lisans 3.( ) Lisans 4.( )Lisans Üstü
5.Göreviniz.
1.( ) Başhemşire /Başhemşire Yardımcısı 2.( ) Başhekim/Başhekim Yardımcısı 3()Müdür/Müdür Yardımcısı
6.Toplam İş Tecrübeniz.
1.( )1 yıldan az 2.( )1-5 yıl arasında 3.( )6-10 yıl arasında 4.( )10 yıldan fazla
7.Mevcut İş Yerinde Çalışma Süreniz.
1.( )1 yıldan az 2.( )1-5 yıl arasında 3.( )6-10 yıl arasında 4.( )10 yıldan fazla

Teşekkür Ederiz

EK 4: SBE TEZ DEĞERLENDİRME FORMU (Jüri Üyeleri İçin)

ÖĞRENCİ BİLGİLERİ

Adı : _____ **Anabilim/Bilim Dalı :** _____

Soyadı : _____ **Programı** : _____

Öğrenci No: _____ **Yüksek Lisans** / **Doktora**

Tez Kodu : _____ ☐ ☐

Danışmanı : _____
İkinci Danışmanı (Varsa) **:** _____

TEZ BAŞLIĞI
:_____

SUNUM	**Tez başlığı çalışma konusunu açık ve yeterli olarak tanımlamakta mıdır?** ☐ Evet ☐ Düzeltilmesi Gerekir
	Tez kolaylıkla okunup anlaşılıyor mu ? ☐ Evet ☐ Kısmen düzeltilmesi gerekir ☐ Yeniden yazılması gerekir
	Tablo, şekil ve grafikler tez yazım kurallarına uygun olarak hazırlanmış mı ? ☐ Evet ☐ Düzeltilmesi gerekir
	Kaynaklar Dizini ☐ Doğru ☐ Hatalı Açıklayınız:
BÜTÜNLÜK	Tez bölümleri birbirlerine mantıksal ve analitik bir bütünlük ve akış içinde bağlanıyor mu? ☐ Evet ☐ Hayır Açıklayınız :
ÖZGÜNLÜK ve YARATICILIK	Aday, sizce bu çalışma sonunda bilimsel araştırma yapma, bilgiye erişme, değerlendirme ve yorumlama yeteneği kazanmış mıdır? ☐ Evet ☐ Hayır Doktora tezleri, ayrıca aşağıda belirtilen niteliklerden en az birini sağlamalıdır. Bu tez çalışması : ☐ Bilime yenilik getirmiştir ☐ Yeni bir bilimsel yöntem geliştirmiştir ☐ Bilinen bir yöntemi yeni bir alana uygulamıştır
GİRİŞ	Araştırmaya konu olan problem tanımlanmıştır: ☐ Evet ☐ Hayır Problemin çözümüne yönelik hipotez/hipotezler açık olarak belirtilmiş ya da araştırma soruları tanımlanmış mıdır? : ☐ Evet ☐ Hayır
GENEL BİLGİLER (Literatür Bilgisi)	Literatür bilgileri özümsenerek derlenmiş midir? ☐ Evet ☐ Hayır Görüşlerinizi **Tez Değerlendirme Kriterleri**'ne uygun olarak belirtiniz

GEREÇ ve YÖNTEM	Görüşlerinizi Tez Değerlendirme Kriterleri'ne uygun olarak belirtiniz:
BULGULAR	Görüşlerinizi Tez Değerlendirme Kriterleri'ne uygun olarak belirtiniz:
TARTIŞMA	Görüşlerinizi Tez Değerlendirme Kriterleri'ne uygun olarak belirtiniz:
SONUÇ VE ÖNERİLER	Sonuç/sonuçlar net olarak belirtilip baştaki hipotez ve/veya araştırma soruları ile ilişkilendirilmiş midir?
KAYNAKLAR	Kaynaklar uygun yazılmış mı? Yeterli mi? Güncel kaynak var mı?
EKLER	Eksik var mı? (Doktora tezleri için makale kabul yazısı ve makale metni), tüm tezler için etik kurul onayları, Arbis formatında özgeçmiş ve yayın listesi
DİĞER	Tez hakkında önemli gördüğünüz diğer hususları bu kısımda belirtebilirsiniz:
JÜRİ DEĞERLENDİRME SONUCU	Tarafımdan incelenen bu tez, Dokuz Eylül Üniversitesi Lisansüstü Eğitim-Öğretim ve Sınav Yönetmeliği uyarıca: ☐ Kabul edilebilir niteliktedir. ☐ Ek süre verilerek düzeltilmesi gerekir. ☐ Ret edilmesi gerekir.

JÜRİ ÜYESİNİN

Adı Soyadı : _____

Anabilim /Bilim Dalı : _____

Üniversitesi/Enstitüsü :_____

Tarih: _____ İmza:

Bu form, Tez Savunma Sınavı'ndan sonra, Sınav Tutanağı ile birlikte en geç üç işgünü iç ilgili Anabilim Dalı tarafından Sağlık Bilimleri Enstitüsü Müdürlüğü'ne gönderilir.

T.C.
İZMİR VALİLİĞİ
İL SAĞLIK MÜDÜRLÜĞÜ

T.C.
İzmir Valiliği
İzmir İl Sağlık Müdürlüğü
(Giden Evrak)
08.03.2011 09:46:11 / 24758
KAMU YATAKLI
Kayıt yapan : AYŞE ÖNCEL

SAYI : B.10.4.ISM.4.35.00.47/ 1002
ŞUBE : Kamu Yat.Ted.Kur.Şub.
KONU : Başak GERÇEKER'in Uygulama İzni

DOKUZ EYLÜL ÜNİVERSİTESİ
SAĞLIK BİLİMLERİ ENSTİTÜSÜ MÜDÜRLÜĞÜ

İlgi: 01/03/2011 tarih ve 595 sayılı yazınız.

İlgi sayılı yazınız Müdürlüğümüzce değerlendirilmiş olup, söz konusu uygulamanın listede adı geçen kamu hastanelerinde yapılması tarafımızca uygun bulunmuştur.

Bilgilerinizi ve gereğini rica ederim.

Uz.Dr.Ahmet Murat IŞIL
Müdür a.
Sağlık Müdür Yardımcısı

S.B.İzmir İl Sağlık Müdürlüğü Kamu Yataklı Tedavi Kurumları Şub.Müd.Hürriyet Bulvarı No:1 Çankaya/İZMİR
Tel: (232) 441 81 11 Faks: (232) 445 43 13 E-Posta: kamu.tedavi@ism.gov.tr

ÖZEL TINAZTEPE HASTANESİ

SAYI: 209

10.03.2011

KONU: Başak GERÇEKER

DOKUZ EYLÜL ÜNİVERSİTESİ
SAĞLIK BİLİMLERİ ENSTİTÜSÜ MÜDÜRLÜĞÜ
İZMİR

İLGİ: 01.03.2011 tarih ve B.30.2.DEÜ.0.42.72.00 / 0595 sayılı yazınız.

Sağlıkta Kalite Geliştirme ve Akreditasyon Yüksek Lisans programı öğrencisi Başak GERÇEKER'in "Sağlık Kuruluşlarında Örgüt İklimi ile Bilgi Güvenliğinin ilişkisi" isimli tez çalışmasını 01 Nisan 2011 – 30 Mayıs 2011 tarihleri arasında Kurumumuzda uygulama yapabileceği izni onaylanmıştır.
Bilgilerinize arz ederiz.

Dr.Ecegül ALBAY BENGİ
Özel Tınaztepe Hastanesi
Mesul Müdür Yardımcısı

DOKUZ EYLÜL ÜNİVERSİTESİ
SAĞLIK BİLİMLERİ ENSTİTÜSÜ MÜDÜRLÜĞÜ
Kayıt Tarihi: 22.03.2011
Kayıt No : 1059
Dosya No :

22.03

203 / 27 sokak No:12 Tınaztepe / Buca - İZMİR
tel: 0 232 454 14 14 - fax: 0 232 454 15 16
www.tinaztepehastanesi.com.tr

ÖZEL KENT HASTANESİ

Tarih : 21.03.2011
Sayı : 2011/361
Konu : Tez çalışması hk.

DOKUZ EYLÜL ÜNİVERSİTESİ
SAĞLIK BİLİMLERİ ENSTİTÜSÜ MÜDÜRLÜĞÜ
İZMİR

İlgi : 01.03.2011 tarih ve B.30.2.DEÜ.0.42.72.00 / 0595 sayılı yazınız.

Enstitünüz Sağlıkta Kalite Geliştirme ve Akreditasyon Anabilim Dalı Sağlıkta Kalite Geliştirme ve Yüksek Lisans programı öğrencisi Başak Gerçeker'in, *"Sağlık Kuruluşlarında Örgüt İklimi ile Bilgi Güvenliğinin ilişkisi"* isimli tez çalışmasını 1Nisan 2011 – 30 Mayıs 2011 tarihleri arasında uygulama yapabilmesi Kurumumuzca uygun görülmüştür.

Bilgilerinize arz ederim.

Saygılarımla.

Dr. M. Ulvi ÜNAL
Mesul Müdür

22.03

DOKUZ EYLÜL ÜNİVERSİTESİ
SAĞLIK BİLİMLERİ ENSTİTÜSÜ MÜDÜRLÜĞÜ
Kayıt Tarihi: 22-03-2011
Kayıt No : 1073
Dosya No :

8229 1 Sokak No: 56 PK: 35580 Çiğli - İZMİR Tel :(0232) 386 70 70 - Fax :(0232) 3
www.kentsaglikgrubu.com - info@kentsaglikgrubu.com

TAPDI BUCA TIP MERKEZİ

Sayı : 339 14 / 03 / 2011
Konu : Başak GERÇEKER tez çalışması

T.C.
DOKUZ EYLÜL ÜNİVERSİTESİ
SAĞLIK BİLİMLERİ ENSTİTÜSÜ MÜDÜRLÜĞÜ

Kurumumuzdan istenmiş olan Başak GERÇEKER'in tez çalışması için onay verilmiştir.
Bilgilerinize.

Dr.F.Gülay UTKANER
TAPDI Buca Tıp Merkezi
Mesül Müdür

EGE SAĞLIK TESİSLERİ VE EĞİTİM MÜESSESELERİ A.Ş.

Kayıtlı Sermayesi : 50.000.000. - TL.
Ödenmiş Sermayesi : 21.613.200. - TL.
Ticaret sicil No. : 31561 K: 377
Ticaret Odası No. : 14936

1399 Sokak No. 25 Alsancak 35220 İZMİR
Tel : (0232) 463 77 00 (Pbx) Fax: (0232) 464 11 88
www.egesaglik.com.tr
egesag@ttmail.com

TARİH : 10/03/2011
SAYI : 173

T.C.
DOKUZ EYLÜL ÜNİVERSİTESİ
SAĞLIK BİLİMLERİ ENSTİTÜSÜ MÜDÜRLÜĞÜ
İZMİR

İLGİ : 01/03/2011 tarih, B.30.2.DEÜ.0.42.72.00 /0595 sayılı yazınız.

İlgili yazınızda belirtilen Yüksek Lisans programı öğrenciniz Başak GERÇEKER' in 1 Nisan 2011- 30 Mayıs 2011 tarihleri arasında hastanemizde tez çalışmasını gerçekleştirmesinde herhangi bir sakınca görülmemektedir.

Bilgilerinize sunarım.

Dr. Bülent ERGÜL
Mesul Müdür