

**T.C.**  
**ATILIM ÜNİVERSİTESİ**  
**SOSYAL BİLİMLER ENSTİTÜSÜ**  
**İŞLETME ANABİLİM DALI**  
**İŞLETME YÜKSEK LİSANS PROGRAMI**

**TÜRKİYE'DE İNSAN KAYNAKLARI YÖNETİMİNDE BİLGİ**  
**GÜVENLİĞİ UYGULAMALARI**

**Yüksek Lisans Tezi**

**Merve ÜNVER**

**ANKARA – 2019**



**T.C.**  
**ATILIM ÜNİVERSİTESİ**  
**SOSYAL BİLİMLER ENSTİTÜSÜ**  
**İŞLETME ANABİLİM DALI**  
**İŞLETME YÜKSEK LİSANS PROGRAMI**

**TÜRKİYE'DE İNSAN KAYNAKLARI YÖNETİMİNDE BİLGİ**  
**GÜVENLİĞİ UYGULAMALARI**

**Yüksek Lisans Tezi**

**Merve ÜNVER**

**Tez Danışmanı**

**Prof. Dr. İsmail BİRCAN**

**ANKARA – 2019**

## **KABUL VE ONAY**

Merve ÜNVER tarafından hazırlanan “Türkiye’de İnsan Kaynakları Yönetiminde Bilgi Güvenliđi Uygulamaları” başlıklı bu alıřma, 10/09/2019 tarihinde yapılan savunma sınavı sonucunda başarılı bulunarak jürimiz tarafından İşletme Anabilim Dalı’nda İşletme Programı Yüksek Lisans Tezi olarak oy birliđi ile kabul edilmiştir.

Prof. Dr. Dilaver TENGİLİMOĐLU (Bařkan)

Prof. Dr. İsmail BİRCAN (Danıřman)

Prof. Dr. Belgin AYDINTAN (Üye)

## ETİK BEYAN

Atılım Üniversitesi Sosyal Bilimler Enstitüsü Tez Yazım Yönergesi'ne uygun olarak hazırladığım bu tez çalışmasını;

- Akademik ve etik kurallar çerçevesinde hazırladığımı,
- Tüm bilgi, belge, değerlendirme ve sonuçları bilimsel etik ve ahlak kurallarına uygun olarak sunduğumu,
- Tez çalışmasında yararlandığım eserlerin tümüne atıfta bulunarak kaynak gösterdiğimi,
- Bu tezde sunduğum çalışmanın özgün olduğunu bildirir,

Aksi bir durumda aleyhime doğabilecek tüm hak kayıplarını kabullendiğimi beyan ederim.

10.09.2019

Merve ÜNVER

## ÖZET

ÜNVER, Merve . Türkiye’de İnsan Kaynakları Yönetiminde Bilgi Güvenliği Uygulamaları, Yüksek Lisans Tezi, Ankara, 2019

Bilgi güvenliği, bilişim sistemlerinin hızla gelişmesi, bilgi ve iletişim teknolojilerinin kullanımının yaygınlaşması ve 'bilgi toplumu' kavramının benimsenmesi ile önem kazanmaya başlayan bir kavram haline gelmiştir. Türkiye’de devlet desteğiyle birlikte hem kamu hem de özel kurumlar için bilgi güvenliği uygulamaları mevzuatlarda yerini almış ve uygulamaya başlanmıştır. Bünyesinde gizlilik, bütünlük ve erişebilirlik unsurlarını barındıran bilgi güvenliği, bu üç unsur çerçevesinde şekillenir. Güvenlik zafiyetinin oluşması için bu üç önemli unsurda eksiklik veya aksaklık olması söz konusudur. Bilgi güvenliğinin var olması için insan faktörü ele alınması gereken önemli bir unsurdur. Bünyesinde insan unsurunu temel alan ve bir değer olarak algılayan insan kaynakları yönetimi, çalışanların kişisel bilgilerine sahip çıkmak, bilgilerini korumak ile sorumludur. Bu nedenle, bilgi güvenliğinin sağlanabilmesi ve güvenlik zafiyetinin ortadan kaldırılabilmesi için uygulanan politikalar, insan kaynakları yönetiminin de uygulaması gereken politikalar dahilindedir.

Bu tezin amacı yapılan değerlendirme sonucunda, Türkiye’de insan kaynakları yönetimi bilgi güvenliği uygulamalarının iş hayatında var olması ve güvenlik zafiyetinin oluşmaması için belirlenmesi gereken stratejileri ortaya koymaktır. Tez çalışmasında bilgi güvenliği ve insan kaynakları yönetimi alanlarında yapılmış çalışmalar, raporlar ve analizlerden faydalanılmış ve tez çalışması 413 insan kaynakları çalışanı ve yöneticisi ile yapılmış olan anket çalışması ile desteklenmiştir. İnsan kaynakları yönetiminde hem çalışanların hem de yöneticilerin bilgi güvenliği konusunda farkındalıklarının artırılması adına eğitim ile bilinçlenmenin meydana gelmesi, insan kaynakları yönetiminde bilgi güvenliği politikası modeli oluşturulması ve bu durumların gerçekleşmesini sağlayacak çözüm önerileri bu tez çalışmasında ele alınmıştır.

**Anahtar Kelimeler:** Bilgi güvenliği, güvenlik zafiyeti, insan kaynakları yönetimi, bilgi güvenliği uygulamaları.

## ABSTRACT

ÜNVER, Merve. Information Security Applications at Human Resources Management in Turkey, Master's Thesis, Ankara, 2019.

Recently information security has gained importance with the rapid development of information systems, penetration of information and communication technologies and the adoption of the concept of “information society.” Implementation of information security tools has been included in the body of the current law and has gotten off the ground with government support in Turkey. Information security, which incorporates confidentiality, integrity and accessibility, are shaped in parallel with these three elements. For the information security gap to occur, one or two of these elements must be lacking or be flawed. Human factor is an important issue that is necessary to address in order to provide information security. Human resources management, which is based on the human factor and which regards “human” as a valuable asset, is responsible for keeping the personal information of the staff confidential. For this reason, policies that are pursued in order to provide information security and eliminate security gap are among the policies that human resources management must implement.

This thesis aims to formulate certain strategies that are required in order to ensure the presence of implementation of human resources management information security tools in business life and in order to avoid information gap in Turkey. In this thesis, reports, analyses and studies that have been conducted in the field of information security and human resources management have been used and the thesis was supported by a survey conducted with total 413 human resources employees and managers. In order to raise awareness of both employees and employers of the importance of information security, solutions that could happen the awakening with the education, set the model regarding human resources management information security and that could allow the implementation of these policies which are actualized these conditions, have been proposed in the thesis hereby.

**Keywords:** Information security, information gap, human resources management, implementation of information security tools.



## İÇİNDEKİLER

<b>ÖZET</b> .....	<b>I</b>
<b>ABSTRACT</b> .....	<b>II</b>
<b>KISALTMALAR DİZİNİ</b> .....	<b>VI</b>
<b>TABLolar DİZİNİ</b> .....	<b>VII</b>
<b>ŞEKİL DİZİNİ</b> .....	<b>VIII</b>
<b>GİRİŞ</b> .....	<b>1</b>
<b>BÖLÜM I</b> .....	<b>5</b>
1.BİLGİ VE BİLGİ TEKNOLOJİLERİ.....	5
1.1.Bilgi.....	5
1.2.Bilgi Teknolojileri.....	6
1.3.Bilişim Teknolojileri .....	7
1.4.Bilgi Güvenliği.....	10
1.5.Kişisel Verilerin Korunması .....	12
1.6.Bilgi Güvenliğinin Uluslararası Statüde Önemi.....	13
<b>BÖLÜM II</b> .....	<b>15</b>
2.BİLGİ GÜVENLİĞİ VE TÜRKİYE’DE İNSAN KAYNAKLARI YÖNETİMİNDE BİLGİ GÜVENLİĞİ UYGULAMALARI .....	15
2.1.Türkiye’de Bilgi Güvenliği.....	15
2.2.Türkiye’de İnsan Kaynakları Yönetimi .....	19
2.2.1.Türkiye’de İnsan Kaynakları Yönetimi Uygulamaları.....	25
2.2.1.1.Planlama.....	25
2.2.1.2.Kadrolama .....	32
2.2.1.3.Değerlendirme .....	34
2.2.1.4.Yerleştirme.....	38
2.2.1.5.Koruma .....	41
2.3.Türkiye’de İnsan Kaynakları Yönetimi’nde Bilgi Güvenliği Uygulamaları.....	43
2.3.1.Yönetim Bilgi Sistemi.....	43
2.3.2.Karar Destek Sistemleri.....	45
2.3.3.Veri, Veri Tabanı ve Veri Deposu.....	46
2.3.4.İntranet, İnternet ve Kurumsal Bilgi Sistemleri.....	47
2.4.Türkiye’de İnsan Kaynakları Yönetiminde Bilgi Güvenliği Uygulamaları Değerlendirilmesi .....	48
<b>BÖLÜM III</b> .....	<b>53</b>
3.YÖNTEM .....	53

<i>3.1.1.Araştırma Amacı</i> .....	53
<i>3.1.2.Araştırma Önemi</i> .....	53
<i>3.1.4.Araştırma Problemi</i> .....	54
<i>3.1.5.Araştırma Hipotezi</i> .....	54
<i>3.1.6.Evren ve Örneklem</i> .....	54
<i>3.1.7.Veri Toplama Araçları</i> .....	54
<i>3.1.8.Verilerin Analizi ve Güvenilirlik</i> .....	55
<i>3.2.Bulgular</i> .....	56
<i>3.2.1.Faktör Analizine Yönelik Bulgular</i> .....	56
<i>3.2.2.Demografik Özelliklere İlişkin Bulgular</i> .....	57
<i>3.2.3.Araştırmanın Hipotezine İlişkin Bulgular</i> .....	59
<b>SONUÇ VE ÖNERİLER</b> .....	<b>65</b>
<b>KAYNAKÇA</b> .....	<b>67</b>
<b>EK 1: ANKET FORMU</b> .....	<b>73</b>
<b>ÖZGEÇMİŞ</b> .....	<b>79</b>

## KISALTMALAR DİZİNİ

ABD	: Amerika Birleşik Devletleri
BSI	: Alman Bilgi Güvenliđi Federal Ajansı
DDoS	: Distributed Denial of Service (Dađıtık Hizmet Engelleme)
ENISA	: Ađ ve Bilgi Güvenliđi Ajansı
ETL	: Extract, Transform, Load
FISMA	: Federal Information Security Management Act.
GYSH	: Gayri Safi Milli Hasıla
ISO	: Uluslararası Standart Organizasyonu
İot	: Internet of Things (Nesnelerin İnterneti)
OCSIA	: Siber Güvenlik ve Bilgi Güvencesi Ofisi

**TABLolar DİZİNİ**

<b>Tablo 1.</b> Seçili 12 Ülke Verilerinin 2000 - 2014 Yılları Arası İnceleme Tablosu .....	9
<b>Tablo 2.</b> Faktör Analizi .....	56
<b>Tablo 3.</b> Cinsiyete Göre Dağılım .....	57
<b>Tablo 4.</b> Yaşa Göre Dağılım.....	58
<b>Tablo 5.</b> Eğitim Durumuna Göre Dağılım.....	58
<b>Tablo 6.</b> Medeni Duruma Göre Dağılım .....	58
<b>Tablo 7.</b> Mesleklerine Göre Dağılım.....	59
<b>Tablo 8.</b> Katılımcıların İnsan Kaynakları Yönetiminde Bilgi Güvenliği Uygulamalarına Yönelik Belirttikleri Görüşlerin Cinsiyetlerine Göre Farklılık Analizi .....	59
<b>Tablo 9.</b> Katılımcıların İnsan Kaynakları Yönetiminde Bilgi Güvenliği Uygulamalarına Yönelik Belirttikleri Görüşlerin Yaşlarına Göre Farklılık Analizi .....	60
<b>Tablo 10.</b> Katılımcıların İnsan Kaynakları Yönetiminde Bilgi Güvenliği Uygulamalarına Yönelik Belirttikleri Görüşlerin Eğitim Durumlarına Göre Farklılık Analizi .....	61
<b>Tablo 11.</b> Katılımcıların İnsan Kaynakları Yönetiminde Bilgi Güvenliği Uygulamalarına Yönelik Belirttikleri Görüşlerin Medeni Durumlarına Göre Farklılık Analizi .....	62
<b>Tablo 12.</b> Katılımcıların İnsan Kaynakları Yönetiminde Bilgi Güvenliği Uygulamalarına Yönelik Belirttikleri Görüşlerin Mesleklerine Göre Farklılık Analizi.....	63
<b>Tablo 13.</b> Bilgi Güvenliği Uygulamaları Düzeyleri .....	63

## ŞEKİL DİZİNİ

<b>Şekil 1.</b> İnsan Kaynakları Planlama Süreci.....	28
---	----

## GİRİŞ

Küreselleşme ile ülkeler arasında daha hızlı mal, hizmet, sermaye akımlarının gelişimi sağlanmış olmakla birlikte aynı zamanda ülkelerin finansal, politik, ulusal güvenlik, çevresel, sosyal, kültürel, teknolojik bağlantılarının bireyler veya piyasalar yardımı ile etkileşime geçmesi sağlanmış olur. Bu şekilde hayatın kolaylaşıyor olması insanların teknolojiye, değişime, gelişime olan bağımlılığını arttırmaktadır. Bilgi teknolojilerinin gelişimiyle kendini göstermiş olan bu bağımlılık, bilgi ve iletişim teknolojilerinin güvenli bir şekilde kullanılıp kullanılmadığı sorusunu da beraberinde getirmektedir.

Bilgi teknolojilerinin gelişmesi ile insanların hayatlarını kolay bir şekilde sürdürebiliyor olması, bilgi erişiminin de kolay bir şekilde gerçekleşiyor olmasını akıllara getirmektedir. İş hayatı ele alındığında insanlara hizmetlerin gün geçtikçe daha pratik ve daha hızlı bir şekilde sunuluyor olması, gelişen bilgi teknolojilerinin temelinde yatıyor olan 'insan' için bir tehdit unsuru olarak karşımıza çıkmaktadır. Bilinçli olsun veya olmasın oluşan güvenlik zafiyetlerinin her ne kadar bilgi teknolojileri gelişmiş olsa da kaynağı yine insan unsurudur. Küreselleşme ile kendini gösteren teknolojik gelişimin ortaya çıkmasıyla meydana gelebilecek bir zafiyetin, insanın sürece dahil olmasıyla birlikte kendini göstermesi imkansız değildir. Bu anlamda söz konusu güvenlik tehdidini kontrol altına alabilecek yine insan olacaktır.

İş hayatında 'insan', 'çalışan' unsuru ele alınırken karşımıza çıkan disiplin ise insan kaynakları yönetimi olacaktır. İnsan kaynakları yönetimi, örgütün devamlılığının, bugün ve gelecekte rekabet üstünlüğünü sağlayabilecek örgüt için gerekli insan kaynağının elde edilmesinin, kaynağın sürekliliği olmasının, çalışan performansını arttırmak ile ilgili stratejilerin belirlenip politikaların izlenmesinin sağlanmasının, insan kaynağının yönlendirilmesinin, koordine ve kontrol edilmesinin kurum bünyesinde barındırılmasının bütünüdür(Armstrong, 2000). Endüstri devrimiyle birlikte karşımıza çıkan bu disiplin, küreselleşme ile ekonomik dinamiklerin değişim ve gelişim göstermesi, 'çalışan' olgusunun oluşması ve sanayi toplumunun ortaya çıkması ile kendini göstermeye başlamıştır. Sonrasında gözlenen I. ve II. Dünya Savaşları,

gelişmekte olan ekonomiler doğrultusunda iş hayatında çalışan ihtiyacını da beraberinde getirmiştir. Böylece çalışan emeğine saygı ön plana çıkmaya başlamıştır. Endüstri psikolojisiyle birlikte ortaya çıkan öğrenen organizasyonlar, toplam kalite yönetimi gibi kavramlar bilgi toplumunun temellerini atmıştır(Dunphy, Turner ve Crawford, 1997, s.16(4)). Bu anlamda çalışan, iş hayatında kimlik kazanmaya ve bir değer olarak ele alınmaya başlamıştır. Bilgi değer kazanmaya başlarken 'çalışan' unsurunun da bir o kadar önem kazanıyor olması insan kaynağının, bilgi güvenliğini göz ardı edilemeyecek bir kavram olarak ele almaya başlamasına sebep olmuştur.

Bilgi ve iletişim teknolojilerinin gelişimiyle çalışanın, üzerinde önemle durduğu bir kavram haline gelmiş olan bilgi güvenliği, meydana gelebilecek bir zafiyet ihtimalini akıllara beraberinde getirmiştir. Bilgi güvenliği zafiyeti, bilgi teknolojisinin gelişiyor olmasından ziyade insan unsurunun süreç içerisindeki rolünden kaynaklanabilmektedir(Calder, 2009, ss.23-25). İnsan, bilişim sistem ağını oluşturduğu gibi sistemsel sıkıntı olarak ele alınabilecek birtakım eylemlere (ihmal, sızma, müdahalede bulunmama vb.) de sebep olabilmektedir. Bu tür durumların önüne geçmek için alınması gereken tedbirler, takip edilmesi gereken prosedürler, belirlenmesi gereken stratejiler olmalıdır.

Bu çalışmada Türkiye'de bilginin güvenlik zafiyetini ortadan kaldırabilmek için var olan bilgi güvenliği uygulamalarının İnsan Kaynakları Yönetimi'nde ne ölçüde var olduğu ve ne derece etkin olabildiği incelenecektir.

Bu amaçla tezin ilk bölümünde öncelikle; bilgi, bilgi ve bilişim teknolojileri, bilgi güvenliği ve yönetim sistemi kavramlarının ne anlama geldikleri, kişisel verilerin korunması için ne gibi uygulamaların kurumlar takibinde olduğu ve bilgi güvenliğinin dünyada nasıl bir konuma sahip olduğu ele alınacaktır. İkinci bölümde; dünya gelişmelerine kıyasla Türkiye'de bilgi güvenliği zafiyetinin önüne geçilmesi anlamında kurumların insan kaynakları süreçleri belirtilerek bilgi güvenliği uygulamalarının dikkate alınacağı başlıklar ele alınacaktır. Üçüncü bölümde ise Türkiye'de insan kaynakları süreçlerinde yer alacak bilgi güvenliği uygulamaları belirtilmiş ve bilgi güvenliği uygulamaları madde olarak değerlendirilecektir. Dördüncü bölümde tez

çalışmamın yöntemi, amacı, evren ve örnekleme, veri toplama araçları, veri analiz yöntemi, bulgular paylaşılacaktır.

İnsan Kaynakları Yönetimi merkezinde 'çalışan' yani 'insan' unsurunu barındırır. Çalışanın iş hayatına adım attığı andan itibaren bilgileri, çalışmış olduğu kurum bünyesinde yer alan İnsan Kaynakları çalışanları ve yöneticileri tarafından kayıt altına alınır. Özlük bilgilerinin yanı sıra kariyer, performans, ücret gibi var olan bilgilerin belirli aralıklarla güncelleniyor, değişiyor, değerlendiriliyor oluşu insan kaynakları için bilgi kaynağının zenginleşmesi anlamına gelmektedir. Bilgi zenginleştikçe korunması daha zaruri hale gelir. Bu da demektir ki bilginin var olması ve zenginleşmesi, korunması noktasında büyük bir önem arz eder. Çalışan bilgilerinin korunuyor olmasında çalışmış olduğu kuruma duyacağı güven, iş hayatındaki performans, kariyer, yetenek noktasında çalışanın değer yaratmasına sebep olmaktadır. Bu anlamda bilgi güvenliğinin sağlanıyor olmasının temelinde çalışanın duyduğu güven yatmaktadır. Kurum bünyesindeki bilgilerin korunuyor olması için kurum tarafından politikalar yürütülüyor olması, bünyesinde var olan çalışanlarının bu anlamda kuruma güven duymasını da beraberinde getirmektedir.

Küreselleşen dünyada teknolojinin gelişimiyle birlikte bilgi kaynaklarının değer kazanması ve iş hayatında bilgi güvenliğinin sağlanması noktasında zafiyetin önüne geçilmesi için ortaya çıkarılmış olan uygulamaları hayata geçirmek zaruri hale gelmiştir. Bu araştırma ile birlikte çalışan bilgilerini bünyesinde barındırarak süreçlerini yöneten İnsan Kaynakları çalışanları ve yöneticilerinin, kurum ve çalışana ait bilgilerin güvenliğini sağlayacak uygulamaları dikkate alarak süreçlerin nasıl yönetildiği, bunun için ne gibi faaliyetlerde bulunulduğu ele alınmıştır.





## BÖLÜM I

### 1.Bilgi ve Bilgi Teknolojileri

Bilgi ve iletişim teknolojilerinin gelişimiyle birlikte son zamanlarda üzerinde durulan bir husus olan bilgi, bilgi güvenliği kavramsal olarak ele alınarak bilgi ve bilişim teknolojileri nedir açıklanacaktır. Kişisel verilerin korunması için var olan uygulamalar genel bir bakış açısıyla değerlendirilerek bilgi güvenliğinin uluslararası statüde öneminden bahsedilecektir.

#### 1.1.Bilgi

Bilen varlık olarak adlandırılan özne ile bilinen varlık olarak nitelendirilen nesne arasındaki iletişim doğrultusunda ortaya çıkan üründür. Öznenin yani insanın nesneyi yani varlığı algılaması, algılayarak düşünce elde etmesi, düşünceyi anlayarak yorumlama yapabilmesi ve yorumlama beraberinde yargıda bulunup açıklama yapılabilmesiyle birlikte bilgi ortaya çıkmaktadır(Sönmez, 2014, s.2). İnsan birden çok konu hakkında düşünüp düşünce doğrultusunda hareket edebilen bir varlıktır. Düşünmek ise insanın farklı soyut ve somut varlıklar ile ilişki kurması ile söz konusudur. İlişki kurmak bu kadar geniş bir yelpaze ise kurulan ilişki doğrultusunda tek bir bilginin ortaya çıkması beklenemez. Bu durumdan bilginin tek bir türü olmamakla birlikte birden çok türünün var olduğu çıkarımını yapmak mümkündür. Gündelik yaşamdan, gerçekleştirilen sanatsal aktivitelerden, bilimsel gelişmelerin var olduğu bir dünyada yaşıyor olmaktan, teknik faaliyetlerde bulunmaktan, yaşanan toplumun bir parçası olan dini yaşamaktan, insanın düşünen bir varlık olmasından dolayı felsefi, sorgulayıcı yapı düşünce yapısının ortaya çıkmasından dolayı birçok farklı bilgi insan yaşantısında var olmaktadır. Bu bilgiler belli bir süreci takip ederek insan hayatındaki yerini sürekli kılmaktadır. Bilgi keşfedilerek bulunur, böylece bilgi açığa çıkmış olur. Açığa çıkan bu bilgi, insan tarafından kaydedilir. Beyinde yer eden bu bilgi kullanılmaya hazır hale gelir ve böylece değerlendirilmeye başlar. Değişen dünyada hiçbir şey aynı kalmaz ve bilgi de aynı şekilde geliştirilerek değişim gösterir. Her şeyden önce insan paylaşılan bir varlık olduğu için bilgi tek bir kişide var olmaz, paylaşılarak var olan insanlara aktarılmış olur.

Bilgi artık vardır, kullanılması gereken durum ve olaylarda başvurulmak üzere arşive kaldırılır.

İnsanların, milletlerin, ülkelerin var olabilmesi ve varlıklarını devam ettirebilmeleri için bilgi çok büyük öneme sahiptir. Bilgi geçmişî günümüze taşıyan, günümüze ve geleceğe yön veren bir kavramdır. Bu anlamda bilginin açığa çıkması, gelişmesi ve aktarılması için insanlara, toplumlara, milletlere, ülkelere büyük sorumluluk düşmektedir. Küreselleşmeyle birlikte kendini gösteren ekonomik, kültürel, siyasal alanlarda ülkelerarası etkileşimin bilgi aktarımıyla gerçekleşiyor olması bilginin değerini arttırmaktadır. Ekonomileri bu denli bilgiye dayanan toplumların bilgi toplumu haline gelmeleri, üretim ve tüketimi de bilgiye dayalı hale getirmiştir. Bilgi teknolojilerinin gelişmesi ile üretimde artışın meydana gelmesi bilgi değerini arttıran bir başka unsur olarak ele alınabilmektedir.

Bilgi bu kadar önemli bir noktadayken korunması da bir o kadar göz ardı edilmemesi gereken unsur olarak karşımıza çıkmaktadır. Bu noktada bilginin korunması ne demektir, bilgi teknolojilerinin gelişimi ile kendini gösteren bilişim teknolojileri bilgi korunması için neleri beraberinde getirmiştir, bilginin güvenliği nasıl sağlanmaktadır, güvenliği sağlayacak sorumlular kimlerdir, ülke sınırlarımızda gerekli değerlendirmeler yapılmadan uluslararası standartlarda bilgi güvenliği nasıl sağlanıyor ele alarak açıklayalım.

## **1.2.Bilgi Teknolojileri**

Toplumsal refahın, bilginin ve insan değerinin önem kazandığı bilgi toplumu, küreselleşme ile ortaya çıkmaya ve de gelişmeye başlamıştır. Bilginin üretilmesi, toplanması, işlenmesi ve korunmasına yardımcı araçlar bilgi teknolojisinin temel unsurlarıdır. Bahsedilmiş olan yardımcı araçlar, her alanda geçerli olmak üzere insan ve bilginin değerini arttırmak için belirlenen hedefler doğrultusunda geliştirilen, takip edilen, uygulamaya konulan teknolojik yapılanmalardır(Tonta, 1999). Bilgi teknolojileri, bilginin oluşmasında verimliliği arttırdığı gibi bilginin paylaşılıp korunmasında da etkinliği sağlamaktadır. Bu durum düzenli olarak yapılan bilgi paylaşımları ve

korumasını otomatik hale getirmeye ve yetkinliklerin keşfedilip bilginin çoğalmasına sebep olmaktadır. Rekabetçi yaşam ve küreselleşme ile gelen kolaylaştırma kavramı yanında bir o kadar da bilgi yoğunluğunun karmaşıklığa sebebiyet verir olması, dünyanın önemli bir parçası olan insan için hayatı sürdürebilmek adına nitelikli bilgiye ulaşma ve o bilgiyi kullanma zorunluluğunu beraberinde getirmiştir. Bilgi teknolojilerinin bilgiye daha kolay erişim sağlıyor olması, bilginin nasıl yönetilebileceğini, nasıl kolay kullanılabilirliğini, nasıl yorumlanabileceğini, nasıl güvenli paylaşılabilirliğinin de cevaplarını beraberinde getirmektedir.

İnternet teknolojisinin yaygın kullanımı ile neredeyse her ev ve iş yerine bilginin giriyor olması hayatın dinamiklerinde yer alan bilginin yerini sağlamlaştırmıştır. Bilginin oluşmasını sağlamak, oluşan bilgiyi işlemek, bilgiyi saklamak, bilgi teknolojisiyle birlikte bilişim sisteminin de sorumluluk alanına girmiştir. Teknolojinin gelişimiyle birlikte bilgisayar gibi teknolojik araçlar, bilginin üretilmesinden paylaşılmasına kadar her süreçte gerekli kayıtları bünyelerinde barındırarak erişimi daha da kolaylaştırmaktadır. Aynı zamanda bu durum bilginin daha hızlı ulaşımını, daha güvenilir olarak saklanmasını da beraberinde getirmektedir. Bu anlamda karşımıza çıkan bilişim teknolojileri kavramına daha yakından bakarak bilgi ve korunması hakkında daha geniş açıdan bakış açısına sahip olmuş olacağız.

### **1.3.Bilişim Teknolojileri**

Bilgi teknolojilerini de kapsayan bilişim teknolojileri, bilginin oluşumundan toplanmasına, işlenmesinden depolanmasına kadar olan süreci ağlar aracılığıyla ilk kullanıcıdan son kullanıcıya iletip bilgiyi yazılım, donanım, veri, ses iletişimi, ağ sistemleri ile kullanıcıların hizmetine sunmada yer alan bütün teknolojilerdir(Grover, Fiedler ve Teng, 1999, s.30). Buradan yola çıkarak diyebiliriz ki iletişim araçları ve bilgisayarlar bilişim teknolojileri dahilinde yer alan önemli teknolojik ürünlerdir. Toplum bilişimin önemli bir tarafı iken toplumun bilgisayar kullanarak anlaşılması güç bilgileri okunabilir şekillerde ortaya çıkarıp depo edebilmesi, bilişim teknolojilerinin topluma ışık tutarak ne kadar önemli bir rol üstlendiğini göstermektedir. Bu anlamda bilişim teknolojileri ülkelerin gelişmelerini etkileyecek önemli bir unsur olarak karşımıza

çıkılmaktadır. Bilişim teknolojisinin altyapısında her ne kadar bilgisayar ve diğer iletişim araçları yer alsada bilgi ve bilgi teknolojisi bütünleşmesiyle oluşan bilişim toplumu, insan unsurunu merkezinde barındırır. Bilgisayar yazılımının, donanımının, ağ sistemlerinin kurulması, geliştirilmesi, ses iletişiminin, veri girişlerinin sağlanması için insana ihtiyaç duyulmaktadır. Bu teknolojilerin aslında insan zekasının yansıması olduğu da göz ardı edilmemelidir.

Bilişim teknolojileri, yapı taşını oluşturan bilgiye istenildiği zaman ve kolay bir şekilde ulaşılmasını gerçek kılarak yeni bilgilerin keşfedilmesini sağlamaktadır. Bu anlamda yeni bilgi yeni insan yeni toplum yapılanması oluşarak toplumun şekillenmesi sağlanabilmektedir. Toplumsal yapının değişmesiyle birlikte ekonomik, siyasal, kültürel yapının da değişmesi söz konusu olmaktadır. Bu anlamda toplumların bilişim teknolojilerindeki gelişime ayak uydurması, toplumsal dinamiklerin güçlenmesine ve toplumların büyüüp gelişmesine olanak sağlamış olacaktır(Cortada, 1998, ss.1-68). Küreselleşme ile birlikte hızla gelişim gösteren bilişim teknolojileri, toplumların diğer toplumlar ile etkileşim içinde olmasını sağlayarak bilgiye en akılcı yoldan ulaşılmasına, refahın var olmasına, eğitim, ekonomi, siyaset gibi alanlarda toplumsal kalkınmanın gerçekleşmesine imkan sağlamaktadır. Bu durumu bir tablo ile açıklamak gerekirse:

**Tablo 1.** Seçili 12 Ülke Verilerinin 2000 - 2014 Yılları Arası İnceleme Tablosu

Ülke	Ort. Makale	Ar-Ge Harcama (%)	Ort. Patent Yerel	Ort. Patent Yabancı	Ort. Yüksek Teknoloji İhracatı	GSYH 2014	Nüfus 2014	Ort. Kişi başı Gelir
<i>ABD</i>	224288	2,65	219919	205060	\$174.345.121.252	\$17.419.000.000.000	318.857.056	\$45.661
<i>Japonya</i>	58348	3,28	333512	55620	\$115.875.133.363	\$4.601.461.206.885	127.131.800	\$37.539
<i>Çin</i>	53064	1,42	211388	78628	\$271.607.146.208	\$10.354.831.729.340	1.364.270.000	\$3.373
<i>Güney Kore</i>	18802	3,00	116245	37169	\$88.752.184.975	\$1.410.382.988.616	50.423.955	\$19.490
<i>Almanya</i>	48052	2,57	48209	12185	\$142.330.495.944	\$3.868.291.231.824	80.889.505	\$37.568
<i>Rusya</i>	16034	1,14	26060	11627	\$5.017.180.405	\$1.860.597.922.763	143.819.569	\$8.011
<i>Hindistan</i>	17312	0,82	5930	21880	\$7.023.850.375	\$2.048.517.438.874	1.295.291.543	\$979
<i>İngiltere</i>	50251	1,68	17863	8771	\$66.590.563.951	\$2.988.893.283.565	64.510.376	\$38.279
<i>Brezilya</i>	11157	1,15	4103	17717	\$7.513.981.208	\$2.346.076.315.119	206.077.898	\$7.364
<i>Fransa</i>	33806	2,13	14257	2607	\$80.162.720.891	\$2.829.192.039.172	66.206.930	\$36.242
<i>İsrail</i>	6960	4,14	1415	5457	\$6.184.993.071	\$305.674.837.195	8.125.300	\$26.290
<i>Türkiye</i>	7645	0,68	1905	706	\$1.358.298.469	\$798.429.233.036	75.932.348	\$7.818

**Kaynak:** World Bank Open Data,2016

Tablo 1’de yer alan veriler doğrultusunda görülüyor ki son yıllarda teknolojik ilerleme ülkelerin gelişmesinde belirleyici bir unsur olarak karşımıza çıkmaktadır. Bilişim teknolojisinin uluslararası piyasa şartlarına uyum sağlayarak toplumlarda gelişim göstermesi ve gelişimin günlük hayata da uyarlanıyor olması toplumların

kalkınmasına sebep olmaktadır. Kendini gösteren bu kalkınma ile ekonomik, siyasi, eğitim alanında var olan faaliyetlerin küreselleşmesine de olanak sağlanmaktadır. Özellikle ekonomik yapıda gerçekleşen küreselleşme ile bilişim teknolojilerine yapılan yatırımları arttırmış, uluslararası ölçekte diğer ülkelerin kalkınma oranlarını da etkilemiştir. Ülkeler bu sayede yeni düzenekler, süreçler oluşturarak düşük maliyetlerle küresel ölçekli rekabetlere atılabileceklerdir(World Bank Open Data,2016).

Toplum gelişimini, kalkınmasını bu derece önemli bir oranda etkileyen bilişim teknolojilerinin ortaya çıkma ve gelişmesinin dayanakları nedir incelemek gerekirse; sadece bilgisayar teknolojisini değil birçok teknolojiyi bünyesinde barındıran bilişim teknolojileri, esasında birden çok temele dayanmaktadır. Bilişim teknolojileri kuantum mekaniği, enformasyon kuramı, moleküler biyoloji, oşinografi, ekoloji ve uzay bilimleri gibi bilgi temelli sistemlerden oluşmaktadır(Güvenen, 1998). Teknolojinin bu kadar önemli bilgilere dayanması, bilginin korunması kavramını da göz önünde bulundurmamıza sebep olmaktadır. Bilginin korunmasının sağlanması için nelere dikkat edilmeli, hangi uygulamalar dikkate alınmalı; bu anlamda bilgi güvenliği üzerinde hassasiyetle durulması gereken bir konu olarak karşımıza çıkmaktadır.

#### **1.4.Bilgi Güvenliği**

Bilginin yetki dahilinde olmadan kullanılmasını, değiştirilmesini, ortadan kaldırılmasını kısaca bilgiye karşı gerçekleştirilen her türlü zararlı ve izinsiz eylemi engellemek için bilgi ve bilişimi teknolojileri dahilinde izlenecek strateji ve uygulamalar ile bilginin korunmasını sağlamaktır. Bilginin güvenliğinin sağlanabilmesi için gizlilik, bütünlük ve erişebilirlik unsurlarının var olması gerekmektedir. Gizlilik; bilginin yetkisiz kişilerin eline geçmesini engellemeyi, yetkisiz erişimlerden korumayı ifade etmektedir. Bütünlük; verinin olması gereken şekilde korunmasının, bilginin bozulmasının, değiştirilmesinin, silinmesinin, üstüne yeni bir veri işlenmesinin gerçekleşmesinin önüne geçileceği anlamına gelmektedir. Erişilebilirlik ise erişim yetkisi olan çalışanların yetkileri dahilinde bilgiye her an zamanında, güvenilir şekilde ulaşılabilir ve kullanılabilir oluşunu taşımaktadır(Gürol ve Sağıroğlu, 2006). Bu kavramlar, bilginin yetkisi bulunmayan kişilerin eline geçmemesi, yetkisi dahilinde

olmayan kişilerce değiştirilememesi, yetkili kişilerce bilgiye ulaşabilir olması korumanın sağlanıyor olduğunu göstermektedir. Sağlanamaması durumunda güvenlik zafiyeti gerçekleşmiş demektir ve gerekli önlemlerin alınması gerektiğine işaretir.

Bilişim teknolojilerinin gelişimi ile bilgi güvenliğinin sağlanması birçok alanda gerekmektedir. Ağ, kullanıcı, veri, uygulama güvenliği, kimlik ve erişim, güvenlik yönetimi ile sanallaştırma ve bulut alanlarında sağlanan bilgi güvenlik uygulamaları ile gizlilik, bütünlük, erişim unsurları göz önünde bulundurularak güvenlik zafiyeti önlenmektedir (Esen, 2018).

Bilgi güvenliği, bilginin korunurluğunu, bir arada olunabilirlik ve yetki sahiplerince kolayca erişilebilirliğini sağlayan bir sistemdir. Bu sistem ISO 27001:2013 standardı ile uluslararası platformda kurallaştırılmıştır(ISO/IEC 27001:2013,2013). Bilgi güvenliği yönetim sistemi izinsiz olarak gerçekleştirilen bilginin ortaya çıkarılması, yok edilmesi, değiştirilmesi, zarar görmesi, erişilmesi, gibi işlemlerden korunmasını sağlamaktadır. Günümüzde bilgilerin bilgi ve iletişim araçlarına işlenmesi ile ilgili araçlarda sistemsel güvenliğin sağlanabilmesi esas olmuştur. Bu durum karşımıza ‘bilgisayar güvenliği’ kavramını çıkarmaktadır. Elektronik ortamlarda bilgilerin gizlenmesi ve taşınması anında bilgilerin özleri bozulmadan, yetkili kişilerce bilgiye erişimin sağlanması ile bir bilgi işleme sistemi oluşturma bilgisayar güvenliğini anlatan bir tanım olarak yapılabilmektedir. Etkinliklerin sorgulanması, erişimlerin izlenmesi, değişikliklerin kayıtlarının tutulup değerlendirilmesi, yok etme işlemlerinin sınırlandırılması gibi güvenlik politikalarının bu anlamda belirlenip izlenmesi gerekmektedir.

Kişi ve kurumlar bilişim teknolojilerinden yararlanırken karşılaşılabilecekleri tehditleri değerlendirerek gerekli tedbirlerin alınması bilgisayar güvenliğinin temelini oluşturmaktadır. Bilgi güvenliği yönetim sistemi ise alınması gereken bu tedbirlerin kuruluşların ihtiyaçlarına göre belirlenip alınması için ne tür gereksinimler karşılanmalıdır belirleyerek güvenliğin sağlanmasına katkı sağlayan en önemli sistemdir. Bilgi güvenliği sistemi, bilginin güvenliğini sağlayarak kişi ve kuruluşlara bu anlamda güven veren gerekli güvenlik kontrollerinin yapılmasını sağlamak için



oluşturulmaktadır. Bu sistem, bilginin korunmasını gerektiren bütün sistemlerce ve bilgiyi başkaları adına yöneten kişi ve kuruluşlarca kurulup kullanılması gerekli olan bir sistemdir. Sistem bilgi güvenliğinin sağlanabilmesi için önce bilginin sisteme işlenmesi için güvenli bir giriş prosedürünün planlanması gerekmektedir. Planlama doğrultusunda gerekli uygulamalar saptanarak gerçekleştirilir. Uygulamaların doğru bir şekilde hayata geçirildiği noktada düzenli kontrollerin yapılmasıyla birlikte karşılaşılabilecek risklere karşı önlemler alınır. Bu doğrultuda sisteme en çok işlenen bilgi olan kişisel verilerin güvenliğinin sağlanabilmesi için sistemsel hangi politikalar takip edilmeli, devlet bu anlamda kurumlara hayata güvenilir bir şekilde geçirebilmesi üzere hangi uygulamaları zorunlu kılan politikaları ele almıştır gibi önemli ve hassas içerik barındıran konuların önemle değerlendirilmesi gerekmektedir.

### **1.5.Kişisel Verilerin Korunması**

Kişi ve kurumların bilgilerini işlemek, korumak ve saklamak için kullanımı artmış olan teknolojik araçlar ile bilgi paylaşımını güvenli bir şekilde gerçekleştiriyor olması belli uygulamalar ile mümkün olabilmektedir. Devletin, güvenli paylaşımın gerçekleşmesi için hukuki yoldan hareket ederek adım atması toplum açısından durumun benimsenebilmesini ve uygulamaya geçilebilmesini kolaylaştırmaktadır. Türkiye’de bu anlamda atılan en kuvvetli adım 6698 sayılı Kişisel Verilerin Korunması Kanunu’nun yürürlüğe girmesi olmuştur. Kişi ve kurumlar böylece bilgisayar ve benzeri teknolojik ürününe işleyeceği kişisel verileri kanuna uygun, risklerin önüne geçebilecek nitelikte dijital ortamda işlemeye ve paylaşmaya başlayacaklardır. Kanun ile kimliği belirli veya belirlenebilir gerçek kişiye ilişkin her türlü bilginin kişisel bilgi olduğu kabul edilerek bilgiler ile ilgili süreçler kişisel bilginin işlenmesi olarak ele alınmaktadır. Kanunda yer alan esaslara aykırı olarak bilgilerin işlenmesi yasaklanarak güvenliğinin sağlanması için uygulamaların getirilmesi insanların hak ve özgürlüklerini koruyan bir durum olarak ele alınabilmektedir. Kişinin rızası olmadan bilgisinin işlenemeyecek olmasını şart koşan yasa ile kişilerin bu anlamda etnik köken, ırk, din, mezhep, siyasi düşüncesi gibi unsurlara göre ayırt edilip gözetilerek muamele görmemesi gerektiği belirtilmiştir. Kişisel bilgiyi işleyecek olan sorumlunun yetkili kişiyi bu anlamda bilgilendirmesi

gerektiđi kanun ile net bir Őekilde belirtilmiŐtir. Kanun esaslarına uygun hareket edilmediđi takdirde yaptırımlarla karŐılaŐacađı yine kanun ile ortaya konularak kiŐisel verilerin korunması konusundaki hassasiyetin ve nemin farkına varılmaktadır.

Kanunla birlikte bir baŐka nemli adım atılarak Trkiye’de KiŐisel Verileri Koruma Kurumu kurulmuŐ ve bylece bilgilerin korunması bilinci arttırılmaya alıŐılarak bilgi temelli kurumlar arasında uluslararası rekabet ortamı oluŐturmak iin faaliyetlere baŐlanmıŐtır. Bu anlamda Trkiye dıŐında bilginin gvenliđinin sađlanması konusunun uluslararası statde nasıl ele alındıđını deđerlendirerek bilginin korunması gerektiđinin nemini daha detaylı olarak ele alabilir, inceleyebilir ve bu dođrultuda politikalar takip ederek eylemler alınabilmektedir.

### **1.6.Bilgi Gvenliđinin Uluslararası Statde nemi**

Bilgi gvenliđi, uluslararası statde farkındalıđı yksek ve zerinde hassasiyetle durularak ele alınan bir konudur. Dnya genelinde drt milyara yakın bilgisayar ve internet ađı kullanıcısı bulunmaktadır ve bu nedenle de kullanıcı sayı arttıķa dijital tehdit sayısı da artıŐ gstermektedir. Global Siber Gvenlik kuruluŐu olan ESET, gn getike bilgi retiminin ve retilen bu bilgilerin paylaŐımının arttıđını bununla birlikte beraberinde gelen birok riskin nleminin alınması gerektiđini belirtmektedir. İnsan hatası sonucu gerekleŐen birden ok gvenlik ihlalleriyle birlikte alınan savunma nlemlerinin hibiri tehditlere karŐı yzde yz koruma sađlanamayacađı grlmektedir. Birden ok tehdide karŐı farkındalık sađlamayı ve bylece insanlarda bu anlamda davranıŐ deđiŐikliđi hedefler politikalar ortaya koyan ESET, Avrupa Gvenlik Ayı uygulamasını destekler nitelikte hareket etmektedir.

Avrupa Konseyi tarafından ye olan lkeler, aynı standartlarda kiŐisel verilerin gvenliđini sađlayabilmesi ve lkelerin sınırları dıŐında gvenli bilgi akıŐını gerekleŐtirebilmesi amacıyla hazırlanmıŐ olan KiŐisel Verilerin Otomatik İŐleme Tabi Tutulması KarŐısında Bireylerin Korunmasına İliŐkin 108 Sayılı SzleŐme imzalanarak uygulanmak zere mevzuatlarına girmiŐtir(KiŐisel Verilerin OtomatikleŐmeye Tabi Tutulması KarŐısında Bireylerin Korunması SzleŐmesi, 1981).

Dünya çapında Türkiye'nin yanı sıra kendi bünyesinde kişisel verilerin güvenliğinin sağlanması bilincine sahip olarak bu doğrultuda faaliyetlerde bulunan birden çok ülke bulunmaktadır. İngiltere'de İngiltere Siber Güvenlik ve Bilgi Güvencesi Ofisi (OCSIA) (Cabinet Office, 2010) , Almanya'da Alman Bilgi Güvelik Ajansı(BSI, 2004), ABD'de Federal Bilgi Güvenliği Yönetim Yasası(National Institute of Standards and Technology, 2004), Japonya'da Kişisel Bilgi Koruma Komitesi(National Information Security Policy Council, Japan, 2006) olarak örnekler karşımıza çıkmaktadır.

ESET, Avrupa Ağ ve Bilgi Güvenliği Ajansı (ENISA), Avrupa Konseyi, DG CONNECT gibi kurumlar ortak hareket ederek uluslararası platformda bilgi güvenliğini tehdit edici durumlara karşı politika ve uygulamalar ortaya koyup ortak bilinç elde etmektedir.

Kurumların gün geçtikçe bilinçlenmiş ve bu doğrultuda gerçekleştirdiği faaliyetlerini etkin, aktif bir şekilde uyguluyor olması, yönetim ve dijital danışmanlık şirketi Accenture'un 15 ülkede 19'u aşkın sektörde yıllık 1 milyar dolar ve üstü hasılatı sahip kurumların 4600 siber güvenlik görevlisiyle yaptığı görüşmeler doğrultusunda hazırlanmış olduğu 2018 Siber Dayanıklılık Raporu'na göre 2017 yılında hedefli saldırıların %70'i engellenirken bu oran 2018 yılında %87'ye çıkmış olmasını bizlere göstermektedir. 2017 yılında her üç saldırıdan biri güvenlik önlemlerini aşabiliyor iken 2018 yılında sekiz hedefli saldırının sadece birinin güvenlik duvarını aşabildiği bilgisi ile kurumların faaliyetlerine devam etmesi, güvenlik yatırımlarını arttırması ve yeniliklerin takibinin yapılması gerektiğine ulaşılabilmektedir (Accenture, 2018).

## **BÖLÜM II**

### **2.Bilgi Güvenliği ve Türkiye’de İnsan Kaynakları Yönetiminde Bilgi Güvenliği Uygulamaları**

Türkiye’de bilgi güvenliğinin sağlanması için devletin, kişi ve kurumların izlemiş olduğu politikalara daha detaylı bakılarak bilgiye olan bakış açısının nasıl olduğu, bilgi güvenliğinin sağlanması noktasında var olan bilincin hangi düzeyde olduğu, bilgi süreçlerinin gerçekleştirilmesinde gösterilmesi gereken hassasiyetin ölçüsünün ne olduğu bu bölümde incelenecektir. Bu doğrultuda Türkiye’de insan kaynakları yönetimi ele alınarak var olan uygulamalar değerlendirilecek ve kurumların insan kaynakları yönetimi ile ilgili hangi uygulamalar doğrultusunda hareket ettiği ele alınacaktır.

#### **2.1.Türkiye’de Bilgi Güvenliği**

Bilginin yetkisi dahilinde bulunmayan kişilerce kullanılması, değiştirilmesi, ortadan kaldırılması gibi eylemlerin gerçekleşmesinin önüne geçebilmek için bilgi ve bilişim teknolojileri argümanlarıyla bilginin korunmasını sağlamaktır. Gizlilik, bütünlük ve erişebilirlik unsurları göz önünde bulundurularak güvenlik zafiyetinin oluşmaması için önlemlerin alınması gerekmektedir. Bilgi güvenliği sisteminin oluşması ve standartlar dahilinde sınırlarının belirlenip korunması ISO 27001:2013 standardı ile uluslararası düzeyde kararlaştırılmıştır. Bilgilerin günümüz bilişim sistemleri üzerine işlenip kaydedilmesiyle birlikte gizlilik unsurunun ihlal edilebilmesi söz konusu olurken oluşturulan, işlenen ve kullanılan bu bilgilerin güvenli bir şekilde korunup yönetilmelerini sağlayan ISO 27001 Bilgi Güvenliği Yönetim Sistemidir.(Şen ve Yerlikaya, 2013) Bu sistem, kurumların personel, müşteri, finansal, fikri mülkiyetlerini korumayı amaçlayan uluslararası düzeyde var olan bir sistemdir. Bu sistem ile kurumlar risklerini belirleyerek nasıl risk yönetimi sağlanabileceği konusunda stratejiler belirleyip uygulamaya geçebilmektedirler. ISO 27001 standardının 2005’te yayımlanmasıyla birlikte kurumlarda değişimler gözlenmeye başlamıştır 2005 itibariyle ortaya çıkan Bilgi Güvenliği Yönetimi Sistemi kapsamında kurumların yaptıkları iş, var olan kadroları ve devam etmekte olan iş süreçleri dikkate alınarak belirlenen birim ve faaliyetler yer

almaktadır. İlgili birim ve faaliyetlerin varlıkları yani bilgi, yazılım, servis, prestij, çalışan gibi temelinde yer alan unsurlar belirlenerek karşılaşılabilecek riskler ve tehditler ortaya konmaktadır. Tehditlerin etkileri belirlenerek gerçekleşme olasılıkları saptanır ve varlıklara ait riskler belirlenir. Her yeni uygulama yüklenip başlatıldığında, yeni bir sistem uygulanmaya başladığında ve yeni tanımlamalar yapıldığında tehdit ve riskler tekrardan analiz edilmektedir. Böyle bir yapıyla kendini gösteren ISO 27001:2005 yeni sistemlerin entegre edilmesinin kolaylaşması, risk değerlendirme standardına daha uyumlu hale getirilmesi, özel denetimlere yer verilmesi, hedef ve performans kriterlerine ek maddeler ilave edilerek performansların takibinin öneminin artışı, riskler karşısında alınacak eylemlerin kapsamının genişletilmesi ve yönetimin sorumluluklarında lider özelliğın daha çok ön planda ele alınması gerekliliğın güncellemeyi söz konusu hale getirerek ISO 27001:2013 meydana gelmiştir(Ersoy, 2012). Böylece riskler daha görünür hale gelerek alınacak tedbirler kuvvetlendirilmiş, kurumun itibarı, güveni ve bilgi güvenliğın farkındalığın artırılmış, çalışanın bilgi güvenliğın uygulamaları esnasında sebep olabilecekleri ihlaller azaltılarak oluşabilecek maliyetin daha düşük olmasına olanak sağlanmış, oluşabilecek en ufak bilgi kaybının nasıl telafi edilebileceğın ve sistemin nasıl kurtarılabilceğın noktasında nasıl hareket edilmesi gerektiğın planı oluşturulmuş, mevzuata uygun hareket etme bilinci kazandırılmış, bilgiye daha kolay ve güvenilir erişim olanağın sağlanmış (ISO/IEC 27001:2005, 2005).

Siber Tehdit Durum Raporu'nda da ele alındığın üzere Türkiye'de TSK tarafından teröristlere karşı başlatılan Zeytin Dalı Harekatı muhaberesinde teröristlerin siber savaş yöntemlerine başvurarak toplumu kışkırtma çalışmaları, doğru olmayan bilgilerin yayınlanması ve kurumlara ait internet sayfalarına saldırı gerçekleştirmeleri ülkemizde bilgiye karşı olan tehditlerin ciddiyetini ve bu tehditlere karşı güvenlik zafiyetinin oluşmaması için önlemler alınması gerektiğın ortaya koymaktadır. Benzer şekilde değinilen Hidden Cobra siber saldırı amaçlı faaliyetleri bulunan grubun ülkemizdeki finans kuruluşlarını hedef alıcı sanal saldırılarda bulunmaları, sınırlarımız içerisinde yer alan sanayi tesislerini hedef alıcı İran bilgisayar korsanlarının faaliyetlerini aktif olarak gerçekleştirmeleri gibi açığa çıkan olaylar doğrultusunda stratejik planlar ile harekete

geçilmelidir. Bu duruma ek olarak gerçekleşen mahrem iş ve personel bilgilerinin izinsiz olarak erişiminin siber suç dahilinde gerçekleşiyor olması güvenlik zafiyetinin ciddi anlamda önüne geçilmesinin gerekliliğini göstermektedir (STM, 2018).

Teknolojinin gelişimi ile birlikte İot cihazlarının toplum içerisinde kullanılabilirliğinin ve bilinirliğinin artması, yaygın bir erişim imkanı yakalaması ile kendini göstermesi, bilginin işlenmesi noktasında ele alınacak bir başka bilişim cihazı olarak karşımıza çıkmaktadır. Ülkemizde İot cihazlarının pazar payının gün geçtikçe daha çok büyüyor olması ve diğer cihazlar ile paylaşım içerisinde olması bünyesinde yer alan bilginin, güvenliğinin sağlanabilmesi için koruma önlemleri alınmalıdır. Bu anlamda atılması gereken önemli adımlardan biri İot cihazlarına veri işlenirken veya diğer araçlar ile etkileşim anında eşsiz şifreleme yapılması olmalıdır. Türkiye’de bu konu üstünde hassas bir şekilde hareket eden kurumlar ile bilgi korunması sağlanabilmekte ve bu hususta meydana gelecek insan ihmalkarlığının ihtimalini düşürecek önlemler alabilmektedir (Westerlund, Leminen ve Rajahonka, 2014).

Uluslararası siber güvenlik kuruluşu olan Arbor’un küresel internet yapılanmasının büyük bir çoğunluğuna sahip olan Atlas isimli tehdit izleme altyapısı, 2017 yılında dünya çapında çevrimiçi erişimi engellemeye yönelik 7,5 milyon saldırı kaydetti. Türkiye’de ise günde 475, saatte 20, dakikada 3 DDoS saldırısı yaşandı. Kasım 2016 - Ekim 2017 dönemine ilişkin 13. Yıllık Küresel Altyapı Güvenliği Raporu’na göre, saldırganların hedeflerine ulaşmak için büyük kapsamlı saldırı hacminden uzaklaşarak “nesnelerin interneti (IoT)” olarak adlandırılan internete bağlı cihazları kullanmaya yöneldiğini görüşündedir. DDoS saldırısı nedeniyle gelir kaybına uğrayan kuruluşların oranı 2017 yılında neredeyse iki katına çıkmıştır. Tüm dünyadan 1, 2 ve 3. katman internet servis sağlayıcıların yanı sıra, barındırma, mobil, kurumsal ve diğer ağ operatörlerinin bir karması olan 390 katılımcının yanıtlarına dayandırılan 13. Yıllık Küresel Altyapı Güvenliği Raporu, özellikle DDoS saldırılarının sayısı ve karmaşıklığının artışı ortaya koymaktadır. Rapora göre; kurumsal internet operatörlerinin %57’si, veri merkezi operatörlerinin ise %45’i, DDoS saldırıları nedeniyle internet bant genişliklerinin fazlaca kullanımı ile karşı karşıya kaldı. İnternet

servis sağlayıcıları saldırı yaşarken, şirketler ise gizli uygulama katmanı saldırılarında %30'luk artışa maruz kaldı. Çok boyutlu saldırıların sayısı önceki yıla göre %20 artarak hizmet sağlayıcılarda %59 ve kurumsal katılımcılarda %48'e ulaştı. Araştırmaya katılanların yüzde 57'si saldırıların etkilerinin başında marka itibarına verdiği zararı öncelikli olarak belirtirken, operasyonel harcamalar ise ikinci sırada yer aldı. 10 bin dolar ile 100 bin dolar arasında mali etki belirten katılımcıların oranı 2016'ya göre neredeyse ikiye katlanarak yüzde 56'ya çıktı. Veri merkezi operatörlerinin yüzde 48'i, başarılı bir saldırının ardından en önemli sorunu müşteri kaybı olarak belirtti. Saldırılarda meydana gelen bu artış ile güvenlik hizmetlerine duyulan talep artmaktadır. 2016 yılında dışarıdan siber güvenlik hizmeti alan kurumların oranı %28 iken 2017 yılında bu oran %38'e çıkmıştır.(Arbor, 2018) Bu doğrultuda Dünya'da da Türkiye'de de hizmet sağlayıcı bu kurumlar ile her sektörden var olan kullanıcılar nitelikli siber güvenlik personelleri önderliğinde çalışmalar başlatmaktadır. Kurumlarda belirli periyodlarla siber saldırı tatbikatı yapılmalıdır görüşü kurum hareketlerinde yerini almaktadır.

Ülkemizde de var olan siber tehdit istihbaratı ile kurum ve kuruluşları hedefleyen bilişim teknoloji cihazları bünyesinde yer alan bilgilerin izinsiz, yetkisiz paylaşımları, erişimleri tespit ederek bu doğrultuda stratejiler izlenmektedir. Bilgilerin işlendiği ve paylaşımda bulunabilen bu cihazların elektronik ortamda karşılaşılabilecekleri saldırılara karşı savunmada bulunması için doğru tespitlerin yapılabilmesi, oluşabilecek zararın ve ihlallerin saptanarak yerinde önlemlerin uygulanabilmesi için siber tehdit istihbaratı gerekli bir hal almaktadır. Panemon Enstitüsü tarafından 2015 yılının ocak ayında yayınlanan ve zararlı yazılımlardan korunmanın oluşturacağı maliyetin minimum seviyede gerçekleşmesi, yapılan bir araştırma ile güvenliğin sağlanmasının ne kadar gerekli ve zor olduğu üzerinde durularak istatistiksel olarak değerlendirilmiştir. Bu ankete göre kurumlarda son 24 ayda maddi anlamda %40 oranında bir güvenlik zafiyeti gerçekleştiği saptanmış ve bu anlamda ihlallerin %80'inin siber tehdit istihbaratı ile engellenebileceği bilgisine ulaşılmıştır. Katılımcıların sadece %36'sı şirketlerinin savunmasını güçlü bulup güvenilir olarak değerlendirmiştir. Katılımcıların neredeyse

yarısı elektronik ortamda gerçekleşen bir saldırının sonuçlarını önlemek veya azaltmak için istihbarat verilerine güvenmek gerektiği düşüncesine sahip olduğunu belirtmiştir. Kurumlar, haftada ortalama olarak 16937 saldırının gerçekleştiğini belirten alarmlar almaktadır. Kurumlar, alarmların sadece 3218'ini (%19) güvenilir olarak değerlendirirken yalnızca 705'ini (%4) araştırabilmektedir. Yanlış alarmlara karşılık yılda 1,27 milyon dolar harcandığı ise araştırma ile tespit edilmiştir. Araştırma sonunda doğru yapılan siber tehdit istihbaratı ile saldırılar karşısında daha yapıcı önlemlerin alınabildiği, saldırıların sayısında azalmanın görülebildiği ve bütçe için bu anlamda doğru yönetilebilmesi gerektiği fikirlerine ulaşılabilmektedir(BGA Security, 2018). Ülkemizde etkinliğini kanıtlamış hizmetlerin sunulması ile kurumlar, siber tehdit istihbarat verilerine danışarak bilginin güvenliğinin sağlanması konusunda adım atarak bilinçlenmektedir.

Siber tehdit istihbaratının yanı sıra kendini gösteren siber sigorta kavramı altında faaliyetlerde bulunan kurumlar da bilginin korunması, var olduğu cihazlarda güvenliğinin sağlanması için ülkemizde önem arz etmektedir. Bilgilerin ihlal edilmesine bağlı olarak oluşacak zararlar ve koruma masraflarını, üçüncü kişilerce izinsiz erişimi, sistemsel kodların ve donanımların çalınması gibi risklerin önüne geçilmesi noktasında siber sigorta devreye girerek önlem almaktadır. 2014 yılından itibaren siber sigorta için yapılan masraflar iki milyar doları aşmış bulunmaktadır. Kurumların güvenlik durumları analiz edilerek, öngörülen riskler doğrultusunda sigorta oluşturup bunu ücretlendiren siber sigorta, kurumlarca alınmış olan önlemlerin riskler karşısında yetersiz kaldığı durumda kalıcı hasarların meydana gelmemesini veya oluşacak zararın bir kısmını karşılayarak kurumun tekrar savunma yapabilmesine destek olmaktadır. Ülkemizde siber sigorta yaptırmış olan kurumlar, bilgilerinin güvenliğini sağlamaştırarak saldırıların minimum seviyede üstesinden gelerek hareket etmeye başlamıştır (Aon, 2018).

## **2.2.Türkiye'de İnsan Kaynakları Yönetimi**

Bir kurumun bünyesinde yer alan personeller ile ilgili yönetsel süreçlerden sorumlu o kurumun insan kaynakları bölümüdür. İnsan kaynakları yönetimi, performans



hedeflerine yönelik personelin davranış ve tutumları ile kurumun personele karşı olan yaklaşımı arasındaki sürdürülebilirliği sağlayıcı politikalar oluşturur, bu doğrultuda uygulamalar geliştirerek bir disiplin çerçevesinde iş sürecini idare eder. Personellerin şirket kültürü altında verimli ve hedef odaklı çalışmasını amaçlamak ile birlikte insan kaynakları yönetimi işgücü planlamasının hedefler doğrultusunda gerçekleştirilmesi, kurum bünyesinde istihdamın gerçekleşmesinin ve personel performansının doğru değerlendirilip doğru iş ile ilişkilendirilmesinin sağlanması, eğitimin verimli bir şekilde personellerin sahip oldukları yetkinliklere göre etkin bir şekilde sağlanması, ücret ödemelerinin adil bir şekilde gerçekleştiriliyor olması gibi sorumlulukları kurum içinde üstlenmektedir. Bu gibi sorumlulukların yerine getirilmesi insan kaynakları yönetiminin kurum içerisinde etkin bir şekilde sağlanıyor olmasının göstergesidir. Günümüzde her şeyin bilgiye dayalı hale gelmesi ve teknolojinin hayatlarımıza bu kadar derinden yerleşmesi bilinenin yanlışların doğru olarak kabul edilmesine sebebiyet verebilmektedir. Bu anlamda insan kaynakları yönetimi olarak kurumlarda büyük sorumluluk düşmektedir. Organizasyon yapısının, iş tanımlarının güncel bir şekilde oluşturulması ve personel açısından yapılan iş ile performans arasındaki denge ilişkisinin verimli bir şekilde kuruluyor olması insan kaynakları yönetimi için önemli bir görev haline gelmektedir. Ekonomik durumların belirsiz bir seyirde gidiyor ve krizlerin yaşanıyor oluşu da göstermektedir ki insan kaynakları yönetimi uzun vadede işgücü planlarını yapmak yerine küresel eğilim ve rekabet koşulları göz önünde bulundurularak iş planlı çalışmaların yapılması ve meydana gelecek bir değişim doğrultusunda öngörülebilir eylemler barındıran stratejilerin oluşturulması gerektiğiyle ilişkilendirilebilir. Aynı zamanda günümüzde yoğun elektronik ortama katılım ile kendini gösteren elektronik insan kaynakları yönetimi uygulamaları, karşılaşılabilecek riskler ve ihlaller hesaba katılarak güvenlik tedbirleri alınması noktasında zorunluluk gerektirmektedir. Yenilikçi, yaratıcı, çözüm odaklı olarak atılan adımlar ile personele yeni, geliştirici kariyer fırsatları yaratıldığı gibi personel üzerinde oluşabilecek bireysel ve organizasyonel stres unsuru ortadan kalkabilmektedir. Kurumlar yapısal, ilişkisel ve insan sermayelerinden oluşan entelektüel sermayeye vereceği önem ile diğer kurumlardan ayrılabilir, fark yaratabilir, rekabet gücünü arttırabilirler. Kurumun yönetiminde yer alan aynı zamanda

bünyesinde yer alan daha birçok departmanında aynı amaçla bir araya gelip çalışmakta olan personellerin meydana getirdiği insan sermayesinin etkili bir şekilde var olmasını insan kaynakları yönetimi sağlamaktadır(Demirkaya, 2015). Yüksek performans hedefinin gerçekleşmesi ile organizasyonel başarının sağlanmış olması etkili insan kaynakları yönetiminin doğru işe alım, doğru performans hedefleri belirleme, doğru eğitim ihtiyacı belirleme, doğru kariyer planlaması yapabilme, doğru bir şekilde organizasyonel bağlılık oluşturabilme, doğru ve adil bir ücretlendirme ile ödül sisteminin var olabilmesi gibi etkenleri bünyesinde barındırıyor olması gerekmektedir.

İnsan Kaynakları Yönetimi'nin dünyada gösterdiği hızlı değişim ve gelişim ülkemizde de kendisini göstermektedir. Personel yönetiminin kavramsal değişimi ile takip edilen süreçte teorik anlamda zenginleşmiş ve iş hayatında kurumsal bir boyut kazanmış olan insan kaynakları yönetimi, uygulamalarının etkin bir şekilde hayata geçirilmesi ve teorik anlamda tamamlanmış olması ile varlığını ortaya koymaktadır. Ülkemizde belirli dönemlerde siyasi, ekonomik, toplumsal gelişme ve değişimler yaşanmıştır. Bu durum insan kaynakları yönetiminde de değişimlerin yaşanmasına sebep olmuştur. Değişime sebep olan dönemler ele alınarak insan kaynakları yönetimi ve uygulamalarını değerlendirmek gerekirse, ülkemiz için önemli bir dönüm noktası olarak tarihte yerini almış olan 1923, insan kaynakları yönetim süreçlerinin incelenmesi için doğru bir başlangıç yılı olacaktır. 1923 yılında Türkiye Cumhuriyeti'nin kurulması ile yeni bir siyasi, hukuki, ekonomik, kültürel ve daha birçok alanda yenilik adımları atılarak cumhuriyet temellerinin atılması, düzeninin oluşması için çalışmalara başlanmıştır. Siyasi düzene baktığımızda kendini gösteren tek parti dönemi, 21 Temmuz 1946'ya kadar var mecliste varlığını koruyacak ve sonrasında demokratikleşme adına ciddi adımlar atılmaya başlanacaktır. Çalışma hayatına bakıldığında ise Osmanlı döneminden kalan bir düzen karşımıza çıkmaktadır. Osmanlı sarayında yer alan çalışanların dışında yer alan ve devlet memuru olarak adlandırılan bir çalışan sınıfla birlikte tarım ile ilgilenen ve zanaat ile uğraşan çalışan kesim, çalışma hayatının parçasıydılar. Devlet memuru olarak görev yapan çalışanlar, Mülkiye (yüksek rütbeli yönetici ve komutanlar), İlmiye (din, yargı, eğitim vb. alanlarda çalışmakta olan

görevliler), Seyfiye (Komutanlar dışındaki askerler ve yeniçeri olarak adlandırılan görevliler) ve Kalemîye (diğer alanlarda çalışan memurlar) olarak sınıflandırılmaktadır. Devlet adına çalışan memurların 1924 anayasasında yapılan değişiklikler ile hakları, görevleri, nitelikleri, maaşları, atama ve işten çıkma işlemleri gibi durumlar ele alınmış ve bu anlamda bir reform kendini göstermiştir. Bununla birlikte 02.01.1924 Hafta Tatili Kanununun kabul edilmesi ile haftada bir gün izin verilmiş çalışma hayatını düzenleme konusunda önemli bir adım atılmıştır. Ekonomik gelişmelere bakıldığında ise dönemde Avrupa devletlerinin sosyal ve ekonomik düzenlerinde büyük değişikliklere sebep olacak olan 1929 ekonomik krizinin altında ikinci dünya savaşı ile ekonomik yapının iyi bir şekilde yönetilememesi, devletin düzenleyici, müdahaleci rolünü üstlenememiş oluşu yer almaktadır ve bu krizle devlet iktisadi politikaları farklı bir yöne doğru gitmeye başlamıştır. Türkiye’de tahıl ve hammadde fiyatlarının düşüş göstermesiyle ihracatının azalması ve Osmanlı borçlarının ödenme zamanının gelmiş olması ekonomik sıkıntıların meydana gelmesinde önemli rol oynamaktadırlar. Bu durum devlet sermayesinin önem kazanıyor olmasını ve özel teşebbüslerin devlet kontrolü altına alınması gerekliliğini beraberinde getirmiştir. 1929 - 1938 yılları arasında devletin en büyük işveren haline gelip sanayinin gelişmekte olması işçi sınıfının da artmasına neden olmuştur. Bu zaman zarfında memuriyet rejiminde gözlemlenen değişiklik olarak maaş sisteminin yetersiz olduğu bir noktaya gelmesi yasa değişikliğine gidilmesine sebebiyet vermiştir. 1933 - 1934 yıllarında yapılan bir araştırma sonucunda elde edilen verilere göre dönem itibari ile çalışan memur sayısının fazla, çalışma koşullarının personelleri zorlar özellikte ve personel niteliklerinin yapılan iş konusunda yetersiz ve standardın altında çalışma usullerinin var olduğu tespit edilmiştir(Öktem, 1992). 1936’da 3008 sayılı İş Yasası çıkartılarak endüstri ilişkilerinde büyük bir değişim meydana gelmiş ve resmi olarak işçi ve işveren hukuki ilişkileri kurulmuş olmaktadır. Bu yasa ile asgari ücret belirlenmiş, çalışma süreleri sınırlandırılmış, iş güvenliği kavramı ortaya çıkmıştır(Güzel, 1986). 1950’li yıllara bakıldığında ise ABD ile ilişkilerin başlamış ve ‘personel yönetimi’ kavramı iş hayatı literatürüne girmiştir. 1960’lı yıllarda bir disiplin olarak ele alınmaya başlayan personel yönetimiyle birlikte Türkiye’de özel sektör kurumlarının bir kısmında işe alım, iş değerlendirme, eğitim, sosyal yardım, ücret yönetimi gibi konular hakkında

çalışmalar yürütülmeye başlanmıştır(Erçek, 2004). 17.06.1949 tarihli 5434 sayılı T.C. Emekli Sandığı Kuruluş Yasası çıkarılmış ve Emekli Sandığı Yasası ile tüm kamu kurum ve kuruluşlar bu yasaya bağlı hale getirilmiştir(Çevikbaş, 1995). Bu dönemde kendini gösteren maaşların yetersiz, niteliksiz personel çalıştırılması doğrultusunda yapılan işte verimin sağlanamıyor, fazla personelin çalışma hayatında istihdam ediliyor ve atama sisteminin etkin bir şekilde çalışmıyor olması, işin niteliğine uygun olarak belirlenememesi, eğitim politikasının yetersiz kalması kendini göstermiştir. 1951'de Maliye Bakanlığı Tetkik Kurulu'nca hazırlanan 'Devlet Memurlarının Ücret Rejimini Islahı Hakkında Rapor' da memur maaşlarının düzeltilmesi için yasal düzenlemeler ve yapılacak değişikliklerin kapsamı belirlenmeye çalışılmıştır. 1952'de ise 'Devlet Memurlarının Ücret Rejiminin Islahı Hakkındaki Akdeniz Raporu'nda yeniden ücret düzenlenmesi öngörülmüş, kamu - özel kesim ücretlerinde denge sağlanmaya çalışılmış, ücret alt ve üst sınırları belirlenmiş, bölge koşullarına göre ücret teklifleri öngörülmüştür (Öktem, 1992). 13.12.1960 yılında kurulan ve 02.05.1961 yılında fiilen çalışmalara başlayan Devlet Personel Dairesi ile Türkiye'deki personel sisteminin gelişimine katkı sağlanmıştır. Böylece liyakat, ücret sistemi, yolluk kanunu, fazla çalışma ücretleri, sağlık yardımları, eğitim gibi başlıklar ilan edilerek yasalaştırılmıştır(Çevikbaş, 1995). 1960'larda anayasal değişikliklerle Türkiye'de dernekleşme kendini göstermeye başlamıştır. 1961 Anayasası ve 1963 yasal düzenlemeler ile sendikal hakların, 274 ve 275 sayılı sendikalar ve toplu sözleşme ile grev ve lokavt kanunlarının tanınmasıyla iş hayatı gelişmeye başlamıştır. 1960'lı yıllarda başlatılan personel reformu çalışmalarının sonucunda çağdaş personel yönetiminin temelleri atılmaya başlamıştır. 1970 sonrasında ekonomik bunalımların yaşanmasıyla birlikte maaşlarda özellikle memur maaşlarında dengelenme çalışmaları yapılmıştır(Aslan, 2012). 1971'de Personel Yöneticileri Derneği (PERYÖN) kurularak personel yönetimi konusunda ilk mesleki örgüt olma niteliğine sahip olmaktadır. Buna karşın Peryön, çalışmaları doğrultusunda iş hayatı çalışma koşullarında etkin bir şekilde reforma sebebiyet verememiştir(Erçek, 2004). 1980 sonrasında önceki dönemlere benzer şekilde kalıcı çözümler yerine personel yönetimi kararlarıyla düzenlenmeye çalışılmıştır. Memur maaşlarının iyileştirilmesi adına 1982'de 2771 sayılı yasa ile aylık ek göstergeler düzenlenmiştir. Memur maaşları

noktasında IMF'nin devreye girerek stratejiler yürütmesi, kalıcı bir çözüm getirmeyerek tarafların memnuniyetsizliğini ortaya çıkarır nitelikte olmuştur. 1990 yılında kurulan ve 1995'de anayasal güvence altına alınan memur sendikacılığı ile 1990 - 1995 yılları arasında etkin bir örgütlenme sağlanamamış olup memur maaşlarında gerçekleşmiş olan maaş iyileşmeleri için çalışmalar yapılmıştır(Aslan, 2012). 1980'lerin sonu ile 1990'ların başına doğru insan kaynakları yönetimi kavramı Türkiye'de yer edinmeye başlamıştır. İnsan Kaynakları Yönetimi konusunda uzmanlaşmış danışman şirketlerinden Egon Zehnder International ve Hay Group'un da Türkiye'de faaliyetlere başlamış olması dünyada kullanılan teknik ve uygulamaların Türkiye'de bulunan şirketlere aktarılmasını sağlamada büyük bir rol oynamış ve kurumların bünyelerinde personel yönetiminin insan kaynakları yönetimine dönüşümüne sebep olmuştur. 1990'larda kurumlar, performans, işe alım ve seçme, eğitim, geliştirme, kariyer planlama gibi konularda sistematik olarak ilerlemeye ve insan kaynakları yönetimini bünyelerinde geliştirmeye başlamışlardır. 1996 yılında Peryön ile İstanbul Üniversitesi İşletme İktisadi Enstitüsü ortak bir adım atarak İnsan Kaynakları Mesleki Yetiştirme Programı düzenlemeye başlamıştır(Erçek, 2004). Çalışanın sosyal güvenceye sahip olması için 1959 yılında çalışmalara başlanıp 1999 yılında 4447 sayılı İşsizlik Sigortası Kanunu'nun kabul edilmesi, İş ve İşçi Bulma Kurumu ve Devlet Planlama Teşkilatı çalışmaları doğrultusunda önemli bir sonuç olarak karşımıza çıkmakta ve aynı çalışma hayatı için önemli bir adım olma niteliğini taşımaktadır. 2000'li yılların başında İş Güvencesi Kanunu çıkarılmasıyla İş Kanunu'nda önemli düzenlemeler yapılmıştır. Bu durumla beraber eğitim, kariyer planlama, performans değerlendirme gibi alanlarda önemli kurumsal planlamalar yapılmaya başlanmıştır.

Ülkemizde insan kaynakları yönetimi gün geçtikçe daha çok çalışma hayatında etkisini gösterirken ne tür uygulamalarla iş hayatında karşılaşıyoruz, insan kaynakları iş süreçlerinde nasıl karşımıza çıkıyor değerlendirmesini yaparak insan kaynakları yönetiminin önemini açığa çıkarabiliriz.

### **2.2.1.Türkiye’de İnsan Kaynakları Yönetimi Uygulamaları**

Ülkemizde insan kaynakları yönetim uygulamaları, insan kaynaklarının işlevselliği ile şekillenmektedir. İnsan kaynakları yönetimi, kurumun üretim yapabilmesi veya bir hizmet sunabilmesi için gerekli, en önemli faktör olarak nitelendirilen insanı çalışma hayatında her yönü ile inceleyip kurum amaçları ile bütünleştiren ilişkiler kurmasını sağlayıcı hedefler doğrultusunda harekete geçirici faaliyetleri gerçekleştiren, saygı, davranış eşitliği, kurum kültürüne bağlılık, çalışma ortamını iyileştirme gibi unsurlar çerçevesinde yönlendirendir. Bu anlamda insan kaynakları yönetimi, en üst düzey yöneticiden en alt düzey personele, tedarik satın alma, pazarlamadan satış sonrası hizmetlere kadar kurumun her bir sürecinde yer alan personelin süreçlerinin idaresini üstlenmektedir. Küreselleşme ile kurumların uluslararası pazarlarda faaliyet gösterir olmasıyla küresel kurumlaşmanın ortaya çıkması, bilgi ve bilişim teknolojilerinin gelişmesi ile birlikte insan unsurunun önem kazanması, gelişmeler doğrultusunda yeni işgücü profillerinin ortaya çıkması ile yönetimin bu gelişime uygun olarak şekillenmesi, rekabet ile başa çıkabilmek için yeni yöntemlerin geliştirilebilmesi, farklı dil, din, ırka mensup personellerin kurum bünyesinde bir olup aynı amaç doğrultusunda çalışabilmesini sağlayacak stratejilerin benimsenmesi gibi faktörler çerçevesinde insan kaynakları yönetimi etkinliğini sürdürebilmektedir. İlgili faktörler ışığında işlevselliğin sürdürülebilir olması yönetimin hangi maddelerin baz alınarak sağlanabildiği sorusunu da beraberinde getirebilmektedir. İnsan kaynakları yönetim uygulamalarının şu başlıklar altında değerlendirilebiliriz:

#### **2.2.1.1.Planlama**

1960’lı yıllarda personel yönetimi kavramları arasında yer alan insan kaynakları planlaması, uzun süredir varlığını sürdürmemekle birlikte bünyesinde birden çok yaklaşım barındırmaktadır. İnsan unsurunun maliyet olarak değil bir kaynak olarak görülmeye başlaması ile kurumların stratejik hedeflerine ulaşabilmesi amaçlanmaktadır. Bu anlamda mevcut durumda ve gelecekte gerek görülecek nitelik ve sayıdaki işgücünü, istenilen yer ve zamanda istihdam edebilmek için yapılan planlama insan kaynakları

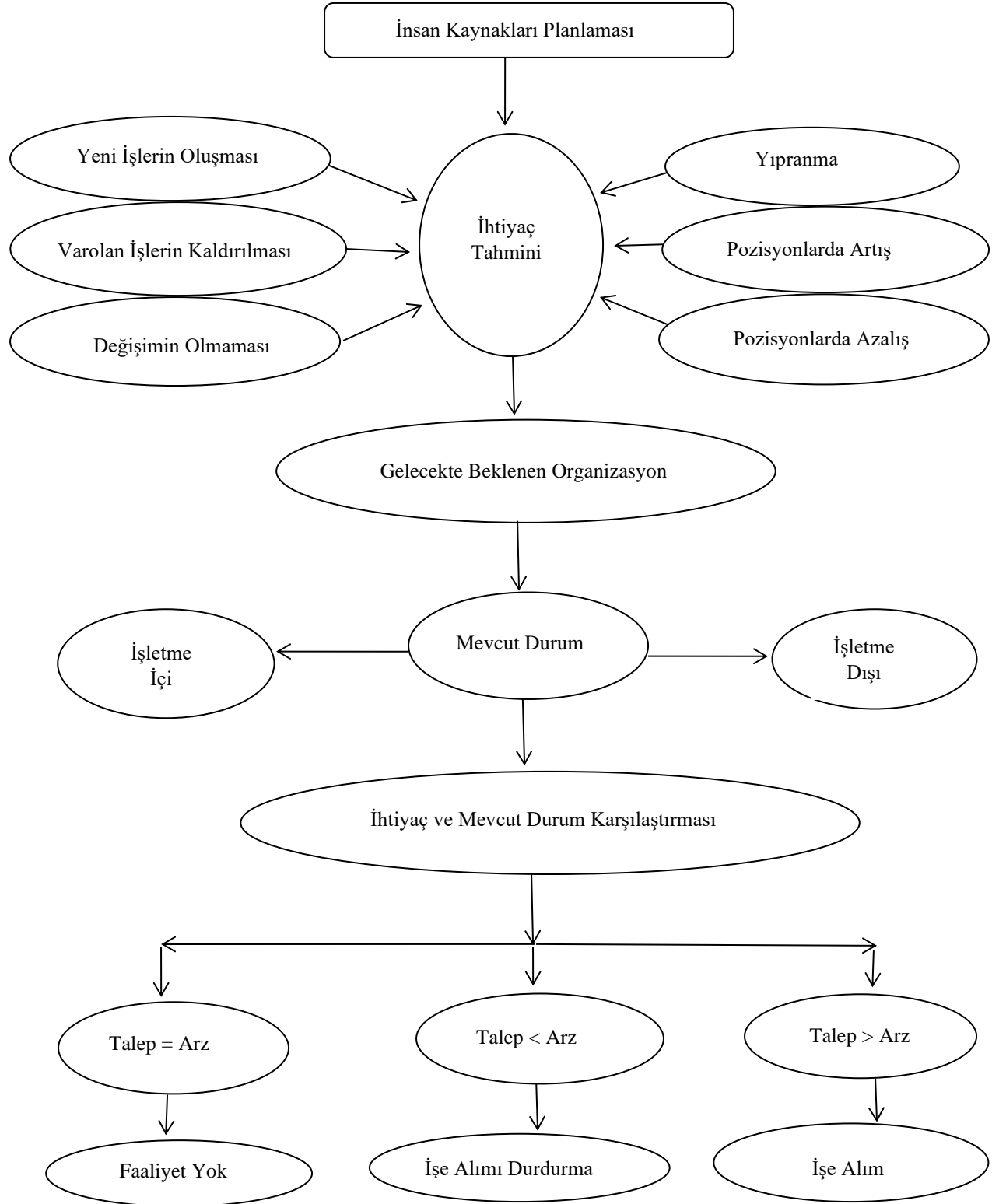
planlaması olarak adlandırılmaktadır. Kurum içerisinde en önemli unsur olarak ele alınan insan üretim süreçleri açısından vazgeçilmez bir unsurdur ve bu nedenle kurumda verimlilik, karlılık hedeflerinin tutturulması için insan kaynakları yönetimi tarafından işgücü planlamasının yapılması büyük bir önem taşımaktadır. İnsan kaynakları planlama süreci aktif bir süreçtir ve devamlılık gerektirmektedir. Doğru zamanda, doğru yerde, doğru yeteneğe sahip işgücünün istihdamı, doğru bir işgücü planlaması yapıldığının göstergesidir. Kurum içerisinde uygun beceri, uzmanlık ve yeterliliğe sahip insan sayısını korumak, insanlarda var olan eksikliklerin ve üstünlüklerin tespitinde bulunarak planlama yapabilmek, değişken çevre şartlarına kurumun daha kolay uyum gösterebilmesini sağlamak için eğitilmiş işgücünü geliştirmek, daha verimli çalışma elde edebilmek için daha esnek çalışma sistemleri geliştirmek ve önemli beceri ve yeteneklere sahip çalışan sayısının az olması durumunda kurum içinde bağlılığın sağlanabilmesi için stratejiler belirlemek bu amaçlardandır(Mathis ve Jacson, 2006, s.44).

İnsan kaynakları planlaması üç aşamada gerçekleşmektedir. İlk aşama, kurumun faaliyetleri esnasında ileride ihtiyaç duyacağı insan kaynağı ihtiyacını belirlemektir. İhtiyaç kaynağının saptanması ile yeni iş alanlarının ortaya çıkması, var olan iş alanlarının ortadan kalkması ya da iş alanlarda değişikliklerin meydana gelmesi mümkün hale gelmektedir. Bu durumlar dahilinde yeni iş kaynağı arayışına veya çalışan sayısının azaltılmasına gidilmektedir. Emekli olacak veya çalışma şartları doğrultusunda iş sözleşmesi feshedilecek çalışanın da belirlenmesiyle insan kaynağı ihtiyacı daha net bir şekilde elde edilebilmektedir. Bu faktörler dahilinde gerçekleşmesi öngörülen iş planı için gerekli insan kaynağı ihtiyacı saptanarak insan kaynakları yönetiminin geleceğe dair yapılanması, faaliyetleri netlik kazanabilmektedir. İkinci aşama ise ihtiyaç duyulan insan kaynağının hangi iş alanı doğrultusunda hangi beceri ve yetkinliklere sahip olması gerektiğinin belirlenmesidir. Kurum içinde ortaya çıkan yeni iş alanlarında devamlılığın ve verimliliğin elde edilmesi için işi yapılabilecek uygun niteliklere sahip çalışanın belirlenmesi, iş alanları arasında uygun yetkinliğe sahip çalışanların transferinin gerçekleşmesi gibi durumlar insan kaynakları yönetimi tarafından planlandığı gibi

kurum dıřında, demografik özellikler göz önünde bulundurularak ilerde duyulacak insan kaynađı ihtiyacı belirlenmektedir. Üçüncü aşamada ise kurum planlarının gerçekleştirilmesi için iş alanlarında olması gerekli yetkinliğe sahip insan kaynađı, doğru yerde doğru zamanda insan kaynakları yönetimi tarafından sağlanmaktadır.

İnsan kaynakları planlama sürecinin her bir safhasında hassas davranılmalı, dikkatli düşünmeli ve analiz yapılmalıdır. Bu anlamda iş tanımlarının oluşturulması esastır.





**Şekil 1.** İnsan Kaynakları Planma Süreci(Mathis ve Jacson, 2006, s.44).

İnsan kaynakları planlaması süreci, ilgili tabloda da görülmektedir ki aşamalı ve analiz doğrultusunda ilerleyen bir süreçtir. Bu süreci etkileyen iç ve dış faktörler bulunmaktadır. Devlet düzenlemeleri, ekonomik koşullar, coğrafi konum, rekabet gücü, iş kaynağının değişmesi dış faktörler olarak ele alınırken; kurum içerisinde iş tanımlarının ve bunun için gerekli iş kaynağı yetkinliklerinin analiz edilmesi, kurumsal yeterlilikler envanteri içsel faktörler olarak değerlendirilebilmektedir. Devlet düzenlemelerini ele almak gerekirse; devletin her bir düzenlemesinin gerekliliklerini bilerek bir insan kaynakları planlaması yapılması kurum ve çalışan açısından büyük önem taşımaktadır. Bu durum gerek kurum hedeflerinin gerçekleşmesine gerek çalışan verimliliğinin artmasına sebep olmaktadır. Ekonomik koşulların değişkenlik göstermesi, ekonomi de yaşanan düşüş veya yükselişlerin yaşanıyor olması insan kaynakları yönetiminin işgücü planlamalarını ihtiyatlı bir şekilde gerçekleştirmesini gerektirmektedir. Enflasyon, faiz oranları, ekonomik kriz gibi etmenler çalışanların kurum içerisinde sayısını ve uygunluğunu belirleyebilmektedir. Bu nedenle ekonomik faktörler göz önünde bulundurularak insan kaynakları planlaması yapılmalıdır. Bununla beraber belirli bir bölgeye yapılan göç, rekabetçi işgücü piyasası şartları insan kaynakları planlamasını etkileyen diğer dış faktörler arasında değerlendirilebilmektedir. Kurumun, diğer kurumun çalışanına sağlamış olduğu sosyal hakları kendi bünyesinde yer alan çalışanına da sağlıyor olması iş kalitesini arttırmakla birlikte rekabetçi işgücü piyasasında kurumun gücünü artırıcı bir nitelik olarak ele alınmaktadır. Yapılan iş doğrultusunda sahip olunması gereken niteliklerin var olmadığı iş kaynağı, insan kaynakları planlamasını olumsuz etkileyen bir başka unsur olarak değerlendirilmektedir. Örneğin yapılan bir iş için çalışanın yaşı, kadın çalışanlar için özel ve iş hayatı dengelerinin sağlanabiliyor olması, kuruma bağlılık gibi özelliklerin aranıyor olması iş planlaması içerisinde de yer almaktadır. İş için gerekli niteliklerin analizi doğru bir şekilde yapılmış olmalıdır, nitelikler doğru tespit edilmeli ve bu anlamda çalışan değerlendirilmelidir. Yapılması gerekli olan işleri ve bu işleri yapacak çalışanın kurum içerisinde istihdam edilip edilmediğini analiz etmek kurum içi faktörlerin insan kaynakları planlamasındaki önemini göstermektedir. Kurumun güçlü ve zayıf yönleri ortaya çıkarılarak ihtiyaç duyulan iş alanlarının belirlenmesi, iş tanımlarının oluşturulması

işgücü planlamasının yapılması için önemli bir başlangıç olmaktadır. Bununla birlikte doğru bir insan kaynakları planlaması için kurumsal yeterliliklerin incelenmesi yani şu an yapılmakta olan işler ile gelecekte yapılması planlanan işlerin doğru bir şekilde anlaşılması ve bu doğrultuda çalışanın ve sahip olduğu yeterliliklerin detaylı bir şekilde analiz edilerek denetlenmesi, çalışan kayıtlarının bu noktada önemli bir veri kaynağı olduğunu göstermektedir. Bilgi, yetenek envanterleri, insan kaynağının gelişim ve işe alım gibi geleceğe yönelik ihtiyaçların belirlenmesinde kullanılarak doğru bir insan kaynakları planlaması yapılabilmektedir. Envanter bilgileri yani çalışanın yaş, çalışma süresi gibi özellikleri, kariyer ilerleyişi, performans değerlendirmesi, gelecekte hangi yeterliliğin hangi iş tanımı için gerekli olacağı ya da hangi iş alanında boş pozisyonların meydana gelebileceği noktasında temel bilgi kaynağı olarak kullanılabilir.

Bir kurum içerisinde kısa, orta ve uzun vadeli iş kaynağı ihtiyacı önemlidir ve bu nedenle insan kaynakları planlaması yapılırken insan kaynağı tahmini ile ilgili geliştirilen tahminler kullanılmaktadır. Bu tahminler, yönetsel tahminler, delfi tekniği, nominal grup tekniği, rasyo analizine dayanan grup tekniği, trend analizi, saçılım grafiği olarak ele alınabilmektedir. Yönetsel tahminler, gerekli insan kaynağını belirleyebilmek için uygulanan tümevarımsal bir yaklaşım olarak değerlendirilmektedir. Kurum içerisinde her bir yönetici, kendi ekibinin verimli bir şekilde çalışabilmesi için birimi dahilinde gerek duyulan insan kaynağının sayısını ve sahip olması gereken yetkinlikleri en doğru şekilde bilendir. Her birim yöneticisi, en alt seviyeden başlayarak planlama süresi içinde birimindeki insan kaynağı ihtiyacını tahmin ederek planlama yapmaktadır. Delfi Tekniği ise kurum bünyesinde birden çok farklı fikrin ortaya çıkmasına sebep oluyorken birimlerdeki uzman kadroyu ortak bir fikirde toplamayı amaçlar. Uzman kadroya yöneticilerinden doldurulması istenen bir anket gönderilir ve anket sorularına verilen cevaplar toplanır. Yöneticiler, uzmanların cevaplarını değerlendirerek yeni bir anket hazırlayıp tekrardan cevaplamaları için anketi uzman kadroya gönderirler. Yeni fikirler ortaya çıkana kadar bu süreç devam etmektedir. Burada amaç sorun çözmektir bu nedenle ankete katılan çalışanların bilgileri saklı tutularak uzmanların fikirlerini değiştirme ve geliştirme fırsatı yaratılmaktadır. Alternatif

beyin fırtınası olarak da adlandırılan nominal grup tekniği, yöneticinin biriminde yer alan çalışanların fikirlerini teker teker olmak üzere alması ile çalışanların fikirlerini yöneticisine sunması beklenmesi tekniğin ilk aşamasını oluşturmaktadır. Yönetici bu fikirleri kaydederek çalışanları bir araya getirir ve tartışma ortamını yaratmış olur. Tartışma sonrası çalışanlar bu fikirlere oy verir ve sonrasında bir sıralama yaparlar. Fikirlerin önceliklerine göre planlama yapılır. Böylece tartışma ile yeni fikirler ortaya çıkmış ve ortak karara varılıncaya kadar fikir üretim, tartışma ortamı oluşması, oy verme işleyişi devam etmiş olur. Kurum bünyesinde yer alan iş alanları ile bu iş alanlarında ihtiyaç duyulan insan kaynağı sayısı geçmiş dönem rasyoların temelinde tahminler yapılarak işgücü planlamasının yapılması karşımıza rasyo analizine dayanan tahmin tekniğini çıkarmaktadır. Bir örnek ile açıklamak gerekirse 200 birim üretim yapabilmek için 10 üretim yapacak çalışana ihtiyaç duyulmuşsa üretim için gerekli üretim yapacak çalışan rasyosu 1:20'dir. 400 birim üretim yapılmak istendiğinde ise 1:20 rasyosuna göre 20 üretim yapacak iş kaynağına ihtiyaç olacaktır ve buna göre işgücü planlaması yapılacaktır. Bir başka insan kaynakları planlamasının yapılabilmesi için ele alınacak teknik olan trend analizinde ise son birkaç yıl içerisinde kurumda gerçekleşen işe alım rakamları arasındaki farklılıklar analiz edilerek iş kaynağı ihtiyacı planlanmaktadır. Trend analizi ile gelecekte ihtiyaç duyulacak çalışan ihtiyacı tahmin edilebildiği gibi analiz verimlilik, satış ve üretim hacmi gibi unsurlardan etkilenmektedir. Bununla birlikte geçmiş ve gelecek işgücü özellikleri ve emeklilik, istifa gibi işten ayrılmalar dikkatli bir şekilde analiz edilerek işgücü ihtiyacı net bir şekilde ortaya konularak insan kaynakları planlaması doğru bir şekilde yapılabilmektedir. Son olarak insan kaynakları planlamasında kullanılan bir analiz yöntemi olarak ele alınan saçılım grafiği ile iki değişken değerlendirmeye alınarak değişkenler arası ilişki analiz edilerek insan kaynağı ihtiyacı tahmin edilebilmektedir. Bir örnek ile açıklamak gerekirse değişkenlerden biri ihracat, bir diğer değişken olarak çalışan sayısı alınırsa aralarında var olan ilişki analiz edilerek ihracatta meydana gelen bir değişiklik çalışan sayısında da değişiklik yaşanmasına sebep olacaktır(Yüksel, 1998).

### 2.2.1.2.Kadrolama

İnsan kaynakları yönetiminde kadrolama süreci, ihtiyaç duyulan insan kaynağının sayı ve nitelikler doğrultusunda aranılarak bulunması ile seçme işleminin gerçekleşmesi ve iş alanlarına seçilmiş olan çalışanın yerleştirilmesi şeklinde gerçekleşmektedir. İnsan kaynağı bulma sürecinde amaç, kurumun ihtiyaç duyduğu nitelik ve ölçüde çalışanın seçilebileceği büyüklükte bir aday havuzunun oluşturulabilmesidir. İç ve dış kaynaklardan yararlanarak ihtiyaç duyulan niteliklere de insan kaynağının bulunmasıyla kurulmuş olan aday havuzundan seçimin yapılması ile insan kaynakları yönetimi seçme süreci tamamlanmış olur. Sürecin tamamlanmasına yardımcı olan iç ve dış kaynakların neler olduğunu ele alırsak; iç kaynaklar, kurum içerisinde yer alan ihtiyaç duyulan iş kaynağı içerikli duyurular ve duyurular doğrultusunda olabilecek başvuruların düzenlemeleri, terfi ve nakil olarak değerlendirilebilmektedir. Kurum içerisinde var olan insan kaynağı ihtiyacı hakkında kurumun bünyesinde yer alan çalışanın bildirim atılan öncelikli bir adımdır. İlgili iş alanlarındaki boş pozisyon ve ihtiyaç duyulan insan kaynağı için aranılan nitelikler hakkındaki bilgiler kurum panosu, kurum bülteni gibi kurum içi iletişim kanalları ile bilgilendirilmeleri sağlanmaktadır. Terfi ise bir çalışanın statü, yetki, ücret bakımından daha üst bir mevkiye yükseltilmesidir. Bu durum, işe yeni girmiş olan çalışan dışında kurum bünyesinde yer alan çalışanların, boşalmış olan pozisyonların istihdamında terfi yöntemine başvurularak değerlendirilmelerine imkan sağlamaktadır. Çalışan performansı, işgücü potansiyeli ve kıdemi terfiinin yapılabilmesi için dikkat edilen önemli kriterlerdir. Bir başka iç kaynak olarak ele alınacak unsur olan nakil ise çalışanın almış olduğu ücret, üstlenmiş olduğu sorumluluk, sahip olduğu yetkileri bakımından bir değişiklik öngörülmeden aynı seviyede var olan boş pozisyona yatay olarak geçişini ifade etmektedir(Muhteşem, 2002, ss.81-87). Birbirine yakın, benzer olan birimlerin görevleri arasında gerçekleşen bir yer değiştirme şeklinde nakil gerçekleşmektedir. Dış kaynaklar ise kurum dışında belirli pozisyon için yapılmış iş duyuruları, insan kaynaklarının bizzat kuruma bırakmış oldukları özgeçmişler, çalışan veya tanıdık insanların belirli pozisyon için aranılan niteliklere sahip olduğunu düşündükleri insan kaynağı tavsiyesi, resmi ve özel iş bulma kurumları, staj uygulaması

olarak ele alınabilmektedir. Aynı zamanda iş kaynağı bulabilmek için çalışan kiralama yani çalışan taşeronluğu yapan kurumlar ile anlaşma, bağımsız çalışan insanlardan yararlanma yöntemlerine başvurularak aranılan insan kaynağı bulunabilmektedir.

İç ve dış kaynakların kullanımı ile istenilen niteliklere sahip insan kaynaklarının, kurum içerisinde havuz oluşturularak özgeçmişlerinin var olması bir sonraki kadrolama süreci olan seçme aşamasını karşımıza getirmektedir. Oluşturulan aday insan kaynakları havuzundan belirli işi en iyi şekilde yapabilmek için sahip olması beklenen bilgi, beceri ve yetkinliklere sahip adayın belirlenmesi seçim aşamasında temel amaçtır. Kurum özgeçmiş havuzundan değerlendirilen başvurular ile ilk görüşme gerçekleştirilir. İlk görüşme sonucunda aday süreçten elensin veya elenmesin, bu görüşme aday odaklı bir yaklaşımla nezaket çerçevesinde yürütülmelidir. Görüşme sonunda belirlenmiş olan işin yapılabilmesi için sahip olunması gereken bilgi ve becerilerin ölçülebilmesi açısından adaylar kurum tarafından yapılacak bir teste tabi tutulur. İlgili testler ölçülecek özelliklere göre çeşitlilik gösterir. Bireysel özelliklere göre testler, grup mülakatları için yapılan testler, sözel olan veya olmayan testler, psikometrik ve projektif testlerin yanında sadece bir özelliği ölçen test olarak özel test, birden fazla özelliği ölçen genel test ve kişiyi bütün olarak değerlendirmeyi amaçlayan test bataryaları test çeşitleri olarak değerlendirilmektedir. Bir testin ölçmeyi hedeflediği özelliği gerçekten ölçer olması geçerli olduğunu kanıtlamaktadır. Bunun yanı sıra testin aynı bireye farklı zamanlarda uygulanmasıyla ele edilen sonucu ile bir önceki test sonucunun benzer olması testin güvenilir oluşunu da göstermektedir. Adaya yapılan testin geçerli ve güvenli olması bu anlamda önem taşımaktadır. Testi olumlu bir şekilde geçen adaylar ile işe alım görüşmeleri yapılmaya başlanır. İşe alım görüşmeleri de amacına göre çeşitlilik göstermektedir. Planlı veya plansız iş görüşmeleri, grup mülakatı, panel tipi görüşme, sorun çözme görüşmesi, stres görüşmesi, ardışık veya sıralı görüşme, karma görüşme olarak iş görüşmeleri ele alınabilmektedir. Planlı veya plansız iş görüşmesi adından da anlaşılacağı gibi ön hazırlığı yapılarak gerçekleşen planlı iş görüşmesi, önceden belirlenmeden gerçekleşen plansız iş görüşmesi olarak adlandırılmaktadır. Bir mülakatçının birden çok adayla gerçekleştirdiği iş görüşmesi grup mülakatı, birden çok

mülakatçının bir aday ile gerçekleştirdiği iş görüşmesi ise panel tipi iş görüşmesi olarak adlandırılmaktadır. Adayların, kendilerine verilen örnek bir vaka doğrultusunda problem çözme ve karar verme becerilerini değerlendirebilmek için yapılan iş görüşmesi sorun çözme olarak adlandırılırken adayın streste olan dayanıklılığın ölçüldüğü iş görüşmesi stres görüşme olarak nitelendirilmektedir. Bir adayın art arda birden fazla görüşmeci ile tek tek görüşme yapması ardışık veya sıralı iş görüşmesi olarak adlandırılmaktadır ve bahsedilmiş olan iş görüşmesi çeşitlerinin birden çok iş görüşmesinde yaşanıyor olması karma iş görüşmesi olarak değerlendirilmektedir. Yapılan iş görüşmelerinde mülakatı gerçekleştiren kişinin önyargı ve kalıp yargılarla adaya yaklaşmaması, adaya karşı kalıp sorular sormak yerine yönlendirici sorularla görüşmeyi sürdürmesi, erken karar vermemesi, adayı doğru bir şekilde dinleme, adayın sadece bir özelliğine bakarak olumlu ya da olumsuz karar vermeme gibi hususlara dikkat etmesi gerekmektedir. Yapılan iş görüşmesi sonunda adayların başvurularında yer alan referanslarının kontrolünün olumlu sonuç vermesiyle adaylar sağlık muayenesinden geçirilir. Adayın fiziksel ve ruhsal yönden işin niteliklerine uygun olması çok önemlidir. Sorunsuz muayene sürecinin atlatılması ile adaylara işe alım için teklif sunulur. İlgili pozisyon için uygun görülen aday ile kurum arasında anlaşma sağlandığı takdirde aday, kurumun bir çalışanı olarak uygun pozisyona yerleştirilerek kurumun kadrolama süreci tamamlanmış olur( Muhteşem, 2002, ss.81-87).

### **2.2.1.3.Değerlendirme**

Kurum içerisinde, çalışanın yaptığı işi nasıl bir performansla tamamlayacağı, yaptığı işte gösterdiği başarının çalışana nasıl bir karşılığı olduğunun veya kurum disiplin kurallarına uyulmadığı takdirde çalışanın nasıl bir prosedüre maruz kaldığı konularının değerlendirilmesi önem taşımaktadır. İnsan kaynağı planlaması, ücret yönetimi, çalışanların eğitim ihtiyacının belirlenmesi, işten ayrılma kararının verilebilmesi gibi konularda karşımıza çıkmakta olan performans değerlendirme sürecini ele almak gerekirse, kuruma sağladığı birçok yararının var olduğunu görebilmekteyiz. İnsan kaynakları planlamasının etkin bir şekilde yapılıyor olması, yönetici - çalışan ilişkisinde iletişimin daha kuvvetli ve sağlıklı olması, çalışanın yöneticisinin

kendisinden nasıl bir performans ile çalışmasını beklediğini kolay anlayabilmesi, çalışanın zayıf ve güçlü yönlerini bilerek kendisini geliştirebiliyor olması, hizmet kalitesinin artıyor olması, kurum karlılığının artıyor olması, eğitim ihtiyacının daha iyi belirlenebiliyor olması gibi yararlar sağlayan performans değerlendirme, beş yöntem ile gerçekleştirilmektedir. Yöntemlerden birisi olan boylandırma yöntemi ile değerlendirmeyi yapan kişi daha önceden hazırlanmış bir çizelge üzerinden her bir çalışana ayrı ayrı değerlendirebilmektedir. Çizelge ile her bir yetkinlik için puanlama yapılarak değerlendirme sonunda puanlar toplanarak çalışanın değerlendirme puanı oluşmuş olmaktadır. Çizelgede yer alan yetkinliklerin yapılan işe uygun olamayarak çizelgede yer alması değerlendirmenin doğru bir sonuca ulaşmamasına sebep olacaktır. Bir diğer yöntem olan sıralama yöntemi, bir birim içerisinde yer alan çalışanlar en iyiden en kötüye sıralanarak değerlendirme yapan kişi, en başarılı çalışana listenin başına ve en başarısız çalışana listenin sonuna yazar ve diğer çalışanlar bu iki çalışan ölçütüne göre değerlendirilir. Çalışan arası karşılaştırmanın yapıldığı bu yöntem basit olduğu gibi çalışanın başarı kriterleri açık ve net olmayabilir. Puan dağıtım yöntemi ise değerlendirme yapılacak birimde yer alan çalışanlara dağıtılmak üzere belirli puanlar verilerek değerlendirme yapacak kişi, çalışan başarısına göre bu puanları dağıtır. Bu şekilde başarı sırası belirlenmektedir. Son yöntem olarak ele alınan zorunlu dağıtım yönteminde ise çalışanlar normal frekans dağılımına göre sıralanmaktadır. Bu duruma göre çalışanların %10'u çok iyi ve çok kötü, %20'si iyi ve kötü, %40'ı ise iyi olarak değerlendirilmektedir (Aldemir, Ataol ve Budak, 2001). Değerlendirmeye alınarak gerçekleşen performans görüşmelerinde hatalar ile karşılaşılabilir. Performans değerlendirme formunun doğru bir şekilde hazırlanamaması, ölçütlerin seçiminde güvenilirlik ve geçerlilik testlerinin yapılmaması, değerlendirme yapan kişinin değerlendirme kriterleri ile ilgili bilgiye sahip olamaması, değerlendiren kişinin çalışanın ile ilişkisinin bozulmamasını ister şekilde aşırı olumlu bir değerlendirme ya da katı bir değerlendirme yapılarak aşırı olumsuz puanların verilmesi, bütün çalışanların ortalamaya yakın şekilde değerlendirilmesi, değerlendirilmenin tek bir ölçüte göre yapılması gibi hataların performans değerlendirme sürecinde yaşanıyor olması kuruma, çalışana sağlayacak olacağı yararları sekteye uğratmaktadır. Performans değerlendirme



sonucunda çalışanın yapmış olduğu işte göstermiş olduğu başarısı, performansı işin gereklerine uygun olup olmadığı değerlendirilir ve böylece başarılı ve başarısız çalışanlar ortaya çıkmaktadır.

Performans değerlendirme süreciyle birlikte başarılı bir çalışma gösteren, yapmış olduğu işi içselleştirerek en doğru şekilde yapmayı amaçlayan ile sadece çalışma süresini bitirmeye odaklı çalışan, yapmış olduğu işte istenilen verimi gösteremeyen çalışanın belirlenmesi, çalışanın başarısı doğrultusunda ödüllendirilmeyle teşvik edilmesini veya olumsuz seyir izleyen performans karşısında uygun disiplin uygulamalarıyla çalışanda yaptığı işe karşı verimlilik artırımı sağlanmasını söz konusu hale getirmektedir. Kurumlarda tehditsel yaklaşımın yerine ödüllendirme sisteminin uygulanıyor olması çalışanda beklenen çalışma veriminin ortaya çıkmasını sağlar ve istenmeyen, iş disiplinine aykırı davranışların gerçekleşmesinin önüne geçilmesine sebep olmaktadır(Salih, 2012). Kurumlarda ödüllendirme dört şekilde gerçekleştirilmektedir. İçsel, dışsal ve performansa dayalı gerçekleşen ödüllendirmede ilk olarak içsel ödüllendirme sistemini ele almak gerekirse; çalışan yapacağı iş için ödül alacağını bilmezken o işi yapmaya başlarsa ve devamını da getirdiği takdirde içsel ödüllendirme sistemi gerçekleşiyor demektir. Çalışanın kendi kendisine bağlamış olduğu ödüllendirme olarak da adlandırılan içsel ödüllendirme, işin gerçekleşmesiyle yaşanan öznel doyumunu ifade etmektedir ve çalışanın kendi denetimi altında gerçekleşmektedir. Çalışanın yapmış olduğu iş ile gurur duyması, işin bir parçası olarak hissetmesi içsel ödüllendirme olarak değerlendirilmektedir. Dışsal ödüllendirme ise çalışanın başarısını dış bir nedene bağlı olarak görmesi ve başkalarının aracılığı ile elde ettiği ödül dışsal ödüllendirme olarak ele alınmaktadır. Bu anlamda ücret, terfi, ikramiye gibi unsurlar dışsal ödül olarak değerlendirilmektedir ve dışsal ödüller yönetici, çalışılan birim ve iş arkadaşları tarafından verilmektedir. Finansal olan ve olmayan olarak açıklanan dışsal ödüllerin çalışanın finansal durumunu değiştirmeden kurumun çalışana vermiş olduğu ödül finansal olmayan, çalışanın finansal durumuna ek bir katkı şeklinde etkisini göstererek kurum tarafından verilmiş olunan finansal olmayan ödül olarak ele alınmaktadır. Finansal olmayan ödüllere örnek olarak esnek çalışma saati imkanı, özel

park yeri tesis etme veya istediği şekilde dizayn edilmiş bir ofis verilirken kardan pay vermek, prim ikramiye veya ücret artırımı finansal olan ödüllere örnek olarak verilebilmektedir. Performans temelli ödüller de performans göstergesi, yeterliliklerin kazanılması veya bunlardan yararlanılması, iş hedeflerinin başarılması, değerlendirme yapma ölçütleriyle belirlenmektedir(Özdemir, 2014). Çalışanın alacağı ücret, gerçekleştirdiği performansın sonucuna bağlıdır. Bu nedenle çalışan, performansının değerlendirilmesinden dolayı ödüllendirileceğini bilerek daha verimli çalışacaktır. Gerçekleşen performans ile hedeflenen performans karşılaştırılarak elde edilen sonucun hedeflenen performans seviyesine yakınlığı, çalışana ödül verileceğinin bir göstergesidir. Kurum içerisinde ödüllendirme olduğu gibi geleneksel ve yapıcı yaklaşım olarak ele alınan disiplinin varlığında da söz edilmektedir. Disiplini, geleneksel yaklaşım cezalandırma olarak ele alırken yapıcı yaklaşım ise çalışanın işine ve çalışma ortamına uyumunu sağlayabilmek için başvurulan yaptırımlar bütünü olarak değerlendirmektedir. İnsan kaynakları yönetiminde çalışanın iş akışına, kurum kültürüne, iş çevresine karşı gerçekleştirdiği yanlış davranışlardan dolayı karşılaştıkları yaptırımlar olarak değerlendirilmektedir. Doğru bir şekilde yönetilen disiplin süreçleri çalışanın performansını olumlu bir şekilde etkileyebilmekte, verimini yükseltebilmekte, hedeflerine odaklanmayı kolaylaştırabilmektedir. Disiplin dört yaklaşımda ele alınabilmektedir. Bu yaklaşımlardan ilki önleyici disiplin yaklaşımıdır ve çalışanın kurum disiplin kural ve düzenlemelerine aykırı bir harekette bulunmaması için yönlendiriliyor olmasını ifade etmektedir. Bu yaklaşımda kontrol söz konusudur ve dış kontrolden iç kontrole geçiş görülmektedir. Yöneticiler, çalışanın etkili bir test ile işe alınmasına, mülakatların açıklayıcı şekilde yapılmasına ve doğru bir şekilde yerleştirilmesine imkan sağlamalı, yapacakları iş için uygun eğitimi almalarını sağlamalı, kurum içerisinde göstermeleri gereken davranışlar konusunda bilgilendirilmelerini sağlamalı, çalışmalarını ile ilgili yapıcı geri bildirimlerde bulunmalıdır. Düzeltici disiplin yaklaşımı ise geleneksel disiplin yaklaşımı olarak değerlendirilmekte ve ceza ile çalışanın disiplinin sağlanabileceği görüşü benimsenmektedir. İş ilişkisinin kesilmesi, ücrette düşüş yaşanması gibi durumların yaşanıyor olması düzeltici disiplin yaklaşımının bir kurumda benimsenmiş olduğunu göstermektedir. Yapıcı disiplin yaklaşımı ise

çalışanın yapmış olduğu yanlış bir davranıştan dolayı cezalandırılmaması görüşünü temel almaktadır. Yaklaşım, çalışana yapılan bir yanlış harekette yol göstermek gerektiğini ve çalışanın bu yanlış hareketi neden yapmış olduğu araştırılarak olumlu bir yaklaşım içinde olmayı, çözüm odaklı yaklaşmayı benimsemektedir. Son olarak ele alınan olumlu disiplin yaklaşımı ise çalışanın yanlış hareket etmesi sonucu yapmış olduğu hareket üzerinde düşünmesi sağlanarak davranışını değiştirme kararı verebilmesi için de bir gün ücretli izinin verilmesi yaklaşımıdır. Bu şekilde çalışanın sakin düşünce ortamına sahip olarak ve iş stresinden uzaklaşarak düşünmesi fırsatı yaratılarak hareketinin nedenlerini daha iyi saptayabileceğini öngörmektedir. Bu sayede çalışanın kurum ile çalışmayı devam ettirip ettiremeyeceği kararını verebilmesine imkan sağlanmaktadır. İzin sonunda çalışan, yapmış olduğu hareketi sürdürmeyeceği düşüncesini çalışmakta olduğu kuruma bildirir, kararına dair imza atar ve bu karar kayıtlara geçilir. Bu durumun tersi olarak çalışan, yapmış olduğu hareketi sürdürmeye kararlı olduğunu çalışmış olduğu kuruma bildirerek kurum ile olan iş ilişkisi sonlandırılmaktadır.

#### **2.2.1.4.Yerleştime**

Oryantasyon, kurum bünyesinde ihtiyaç duyulan nitelikte insan kaynağının seçilip yerleştirilmesiyle birlikte çalışanın işe adaptasyonunun kolay bir şekilde gerçekleşmesi için kurum tarafından yürütülen bir süreçtir. Kurumun kültürünün, hakim olduğu davranış biçiminin, temelinde yer alan fiziki ve sosyal bilgilerin yeni işe başlayan çalışan için öğrenimi, oryantasyon süreci ile gerçekleşmektedir. Kurumu tanıtıcı yayınlar, grup toplantıları, kurum çalışanları ile gerçekleştirilen oturumlar, bireysel görüşmeler, kurumu tanıtıcı geziler gibi yöntemler oryantasyon sürecinin parçalarını oluşturmaktadır. Kurum bünyesine yeni katılmış olan çalışan oryantasyon süreci ile günlük iş akışı, kendisine sağlanacak kurum hizmetleri, kurum politikaları, kurum ürün ve hizmetleri, iş güvenliği uygulamaları gibi bilgilerin edinimi daha kolay bir şekilde mümkün olacaktır (Recordo ve Jolly, 1997).

Çalışan tarafından yapılacak işin en iyi şekilde yapılabilmesi ve bunun için çalışanın ihtiyaç duyacağı bilgi ve becerinin kazanımının sağlanması aynı zamanda çalışma arkadaşlarına, çalıştığı birime ve kuruma uyum sağlayabilmesi, çalışanın terfi edebilmesi için yetkinlik kazandırılması oryantasyon sürecini takip eden eğitim süreci ile mümkün olabilmektedir. Çalışana kurumca sağlanan ve kurum dışı veya içinde gerçekleştirilen eğitimler ile çalışanın yetiştirilmesi ve geliştirilmesi amaçlanmaktadır. Çalışanın yetiştirilmesi, yapılacak olan işin her bir aşamasındaki görevlerin tamamlanabilmesi için çalışana kazandırılması amaçlanan bilgi, beceri ve yetenektir. Verimli bir çalışma ortaya koymak için işin en doğru şekilde yapılacak olması, çalışanın yetiştirilmesindeki en temel amaçtır. Çalışanın geliştirilmesi ise yöneticinin çalışanı, kurumun yapı ve işleyişinin bir parçası olarak görebilmesi, kurum içerisindeki rolünü daha iyi anlayabilmesi ve uygulayabilmesi için eğitime tabi tutulmasının ve geliştirilmesinin desteklenmesidir. Geliştirme süreci dört aşamada gerçekleşmektedir. İlk aşama eğitim analizinin yapılmasıdır. Kurum bünyesinde yer alan birimlerde görev alan çalışanların hangi eğitime ihtiyaç duyduğu, bu doğrultuda hangi eğitimleri alarak başarı elde edebileceği, yapılan işte performansın nasıl arttırılabileceği, yapılacak işin gerektirdiği hangi niteliklerin çalışanda olup olmadığı gibi konular ele alınarak doğru bir şekilde eğitim analizi yapılmaktadır. Analizle birlikte eğitim içerikleri hazırlanır. Eğitim sonuçlarının değerlendirilebilmesi için eğitimin amaçları net bir şekilde belirlenmelidir. Bu doğrultuda ele alınacak olan bir başka aşama ise eğitimin belirli bir amaç ve plan doğrultusunda gerçekleştirilmesidir. Son aşama ise çalışanda verilen eğitim ile yaratılmak istenen bilgi ve davranış değişikliğinin gözlenmesi, değerlendirilmesidir. Eğitim sonucunun değerlendirilmesi için test-tekrar, önceki-sonraki performans ve deney-kontrol grubu yöntemleri kullanılmaktadır. Kurumun çalışanın yetiştirilmesi ve geliştirilmesi için sağlamış olduğu eğitim, iş başı ve iş dışı eğitim olarak ayrılmaktadır. İş başı eğitim, çalışanın çalışma ortamından uzaklaşmadan eğitiminin yapılmasıdır. İş başı eğitim, daha az maliyetlidir, iş sürecini aksatmamaktadır, çalışana öğrenmiş olduğunu daha kolay bir şekilde uygulayabilme imkanı sunmaktadır ve çalışanın çalışma ortamına adapte olabilmelerini sağlamaktadır. Yönetici gözetiminde eğitim, yetki devri ve formen aracılığı ile eğitim, iş rotasyonu, takım çalışması ile eğitim, oryantasyon eğitimi

başlıca iş başı eğitimleridir. İş dışı eğitim ise çalışanın yapmış olduğu işten uzaklaştırılarak belirli bir konuda bilgi kazandırma ve yetkinlik geliştirilmesidir. İş dışı eğitimin çalışırken daha iyi odaklanma, grup halinde yapıldığında maliyet ve zaman kazanımı sağlama, öğrenme için uygun ortamlar, eğitim maliyetini ve süresini kolayca hesaplama gibi özellikleri mevcuttur. Konferans, seminer, kurslar, T grup, örnek olay, rol oynama, işletme oyunu yöntemleri, beklenen sorular, açık hava, simülasyon eğitimleri iş dışı eğitim kapsamında yer almaktadır. Eğitici ve çalışanların farklı ortamlarda yer aldığı e-öğrenme yöntemi ile de kurum bünyesinde çalışana eğitim imkanı sağlamaktadır. Yüz yüze eğitimin benzeri olarak ağ üzerinden sanal ortamda gerçekleşen senkron e-öğrenme ve canlı bir etkileşim olmadan çalışanın çalışma temposunu kendisinin belirlediği asenkron e-öğrenme online olarak gerçekleşen eğitim türleri olarak değerlendirilmektedir( Taymaz, 1981).

Kariyer planlaması ise kuruma kendine belirli bir kariyer yolu belirleyerek başlayacak olan çalışan, bu yolda ilerlemede var olan amacını ve amacını gerçekleştirmek için kullanacağı araçları ifade eden süreçtir. Değişen şartlara uyum sağlamak için beşeri sermayenin geliştirilmesi, kurum yapısında var olan kararlılık ve esneklik özelliklerinin de gelişim göstermesi ile kariyer planlama daha önemli bir konuma gelmektedir. Kurumun uygun kariyer planlama yapması çalışanda verimin artışına, yapacağı işe bağlı hareket edeceğine, yeniliklere açık olacağına, değişimlere daha kolay uyum sağlayacağına sebep olmaktadır. Kariyer planlaması; ulaşılmak istenen hedef ile ilgili genel bir bakış açısına sahip olunması, geleceği olan sektör ve kurumların belirlenerek çalışanın bilgi ve becerilerine göre belirlenen sektörlerin, hedefe dahil edilmesi, çalışanın belirlenen sektör bünyesinde yer alan pozisyonların bilgi ve becerileri doğrultusunda seçilmesi, çalışanın güçlü ve zayıf yönlerinin belirlenerek zayıf yönlerinin en aza indirgenmesinin sağlanması, verilen kararları yerine getirebilmek için hareket planının oluşturulması, finansal yapının belirlenmesi ve yaşanabilecek değişimlere karşı güncel finansal yapının oluşturulması aşamalarından oluşmaktadır. Çalışanların kendi kariyerinde başarısını gerçekleştirebilmesi, insan kaynağının etkin bir şekilde kullanımının, çalışanın geliştirilmesinin ve iş başarısının yükselmesinin

sağlanması, iş güvenliğinin var olması kariyer planlamasının amaçları olarak ele alınmaktadır (Bayraktaroğlu, 2006).

### **2.2.1.5.Koruma**

İş güvenliği, çalışanların kurum içerisinde karşılaşılabilecekleri iş kazalarının önüne geçebilmek için alınan tedbirler olarak ifade edilebilmektedir. Çalışma ortamında iş düzenini geçici veya sürekli bir şekilde durduran kaza iş kazası olarak karşımıza çıkmaktadır. İş kazalarının yaşanıyor olması iş güvenliğinin çalışma ortamında sağlanamadığını göstermektedir. Ülkemizde ‘işçi sağlığı ve iş güvenliği’ olarak bilinen iş güvenliği kavramı, 2012 yılında yayımlanan 6331 sayılı İş Sağlığı ve Güvenliği Kanunu ile ‘iş sağlığı ve güvenliği’ olarak adlandırılmıştır. İş güvenliği ile yapılan işler esnasında iş kazası olma ihtimalini en düşük seviyeye indirmeye, çalışma ortamından kaynaklı oluşabilecek sağlık sorunları ve meslek hastalıklarının önüne geçilme söz konusu olmaktadır. Çalışanın işe başlamadan önceki sağlık durumu ile işe başladıktan sonraki güncel sağlık durumunun aynı olmasının sağlanıyor olması iş güvenliğinin temel amacıdır. Yapılan her iş için alınan iş güvenliği tedbirleri farklılık göstermektedir. Tehlike seviyesine göre sınıflandırılması gereken işlerin bu doğrultuda alınacak tedbir seviyesinin de yükselmesi gerekmektedir(Arıcı, 1999). İş güvenliği uygulamalarına çalışanların katılımı büyük önem taşımaktadır. Bu duruma ek olarak iş güvenliği uzmanları, işyeri hekimleri ve diğer sağlık personelleri katılımı ile iş güvenliğinin teknik işleyişi gerçekleştirilmiş olur.

Çalışan sağlığı ise çalışma ortamında risk altında olmamalıdır. Endüstrileşme ile birlikte çalışanın, yaşamına engel teşkil edecek tehlikelerden, vücut ve ruh sağlığına zarar verici durumlardan korunmasının önemi bu anlamda ortaya çıkmaktadır. Çalışan sağlığının zarar görmesi çalışan açısından gelir kaybı yaşamasına sebep olacağı gibi sakatlık veya ölüm gibi durumlarla da çalışanın karşı karşıya bırakabilmektedir. Çalışanın sağlığı bu kadar önemliyken iş güvenliğinin sağlanabilmesi açısından devlet ve kurumun kendi iç denetim birimi tarafından belirli aralıklarla denetimler, kontroller gerçekleştirilmelidir. Prosedürlere uygun hareket edilmesi, doğru bilgilendirilmelerin

yapılması, bilinç sahibi olunması bu noktada ele alınıp değerlendirilen önemli konulardır. İnsan kaynakları planlamasının eksik bir şekilde gerçekleşiyor olması, değişikliklere uyum sağlama noktasında yetersiz kalınması; kurum içerisinde yaptırım gücünün kaybediliyor olmasına, kurum içerisinde etkileşimin, iletişimin, motivasyonun, desteğin azalmasına sebep olacaktır. Bu durum çalışanda dikkat dağınıklığının, stresin, endişenin ortaya çıkmasına neden olacaktır ve iş güvenliğinin çalışan dolayısıyla sekteye uğramasını söz konusu hale getirecektir. Aynı şekilde iş analizinin yerinde değerlendirmeler ile doğru bir şekilde yapılması, doğru insan kaynağının seçiminin gerçekleşmesi, eğitimin ihtiyaca göre gerçekleştirilmesinin sağlanması, performans değerlendirmenin uygun kriterlere göre gerçekleşmesi, adil ücretlendirme sisteminin var olması çalışanların iş güvenliğini tehlikeye sokabilecek davranışlarda bulunabilmesinin önüne geçebilmektedir.

## **2.3.Türkiye’de İnsan Kaynakları Yönetimi’nde Bilgi Güvenliği Uygulamaları**

İnsan kaynakları yönetimi uygulamaları olarak ele alınan planlama, kadrolama, değerlendirme, yerleştirme ve koruma başlıkları altında değerlendirilen işgücü planlamaları, iş tanımları, analizleri, gerekleri, seçme ve yerleştirme, performans değerlendirme, disiplin ve ödül, oryantasyon, personel eğitimi, kariyer planlama, iş güvenliği ve çalışan sağlığı bünyesinde işlenmiş bilgilerin güvenliğinin sağlanıyor olması önemli bir konu olarak karşımıza çıkmaktadır. İnsan kaynakları uygulamalarının eksiksiz ve aksama yaşanmadan gerçekleşebilmesi için kullanılan geleneksel yöntemlerin bilgi ve bilişim teknolojilerinin gelişimiyle birlikte yetersiz kalması ve emek, zaman kaybının önüne geçilmek istenmesi, internet ve bilgisayar kullanımının insan kaynakları yönetimi çalışanları ve yöneticileri tarafından çalışana ait bilgilerin işlenmesi olarak kullanılmaya başlanmasını gerekli hale getirmiştir. Bilginin sisteme işlenmesi ile ilgili uygulamaları ele alarak bilginin korunmasının nasıl sağlanabileceği hakkında nasıl bir yöntem izlenebileceği belirlenebilmektedir.

### **2.3.1.Yönetim Bilgi Sistemi**

Yönetim Bilgi Sistemi, Çalışanların ve yöneticilerin bilgiye doğru bir şekilde, doğru bir yöntemle ve doğru bir zamanda ulaşabilmesi için kurulan bir sistemdir. Yönetim fonksiyonlarının kolaylaşmasını hedefleyen bu sistem, zaman ve maddiyat tasarrufu ile bilginin interaktif bir şekilde kullanılması amacıyla oluşturulmuştur. Bilgi üzerinde kontrol bu sistem ile sağlanabilmektedir. Bilginin elde edilmesi, değerlendirilmesi, analiz edilmesi, gerekli kullanıcıya zamanında ve doğru bir şekilde ulaşmasını sistem sağlamaktadır. Bilgi gereksinimini sürekli bir şekilde sağlayan sistemin temelinde üç unsur yer almaktadır. Bu unsurlar, yönetim, bilgi ve sistemdir. Karar gereksinimleri saptanır, bilgi sağlama ile destek verilir ve böylece karar verme süreci tamamlanarak yönetim gerçekleşmektedir(Chene, 2009). Doğru bir karar vermenin de temelinde doğru bir bilgi yatmaktadır. Doğru kaynaklardan elde edilen bilgilerin işlenerek farklı bilgi türlerine göre ayrıştırılması, bilginin doğru bir şekilde doğru kişi tarafından kullanılmasına sebep olmaktadır. Doğru bilgi ve doğru bir karar



doğrultusunda belirli bir görevi gerçekleştirebilmek için organize edilmiş çalışanların, makine ve ekipmanların, uygulamaların bütünü ile oluşan sistem ile bilgi, doğru bir şekilde kurum içerisinde var olabilmektedir.

Yönetim bilgi sistemi; karar verme ve yönetimin planlama sürecine katkı sağlar, raporlamayı ve kontrolü esas alır, kurum içerisinde var olan bilgi akışını yönlendirir, analiz ve tasarım ile bilgi ihtiyacını karşılar, bilgi işleme fonksiyonunu destekler, bilgiye kolay ulaşılmasını sağlar, sadece yetki dahilinde çalışanın bilgiye erişimine izin verir. Kolay ulaşım, erişime izin gibi dikkat çeken eylemlerin söz ediliyor oluşu bilgiye ulaşmanın nasıl bir süreç doğrultusunda gerçekleştiği veya erişimin yetki çerçevesinde izin yönetiminin ne kadar etkin şekilde var olduğu sorularını da beraberinde getirmektedir. Bilgiye ulaşmada kullanılan kanal ve sistemlerin güvenilir olması önemli bir konudur. Günümüzde bu anlamda internet çok tercih edilen bir kanal olarak ele alınmakta ve bu durum beraberinde güvenli internet kavramını, erişimin kontrollü bir şekilde gerçekleşiyor olmasını getirmiştir. İnternet bünyesindeki zararlı yazılımların işlenen bilgiyi yetkisizce paylaşması, istenilen bilgiye yanlış kanaldan ulaşarak bilgi kirliliğinin var olması, işletim sisteminin güvenlik duvarlarının olmaması durumlarının önüne geçebilmek için internet aracılığı ile bulunan, kullanılan, kaydedilen bilginin var olduğu bilgisayara veya benzeri depolama biriminde güvenlik duvarının oluşturulması, bilgi erişiminin yetkilendirilmesi ve bu anlamda şifreleme yönteminin kullanılması gerekmektedir(Maguire ve Redman, 2007, ss.252-264).

Günümüzde teknolojinin gelişimi ile birlikte BULUT gibi bilgi işlem platformlarının kurumlarda kullanılarak internet ortamında yer alan bilgisayar bünyesindeki bilgilerin depolanması, başka bir ortama aktarılması sağlanabilmektedir. Kurumlar yazılımlarını bilgisayar ortamından mobil ortama taşıyarak kurum içerisinde bilgi aktarımını hızlandırmakta, kurum iletişimine hız kazandırmakta ve hızlı karar verilebilmesine ortam hazırlamaktadır(Zissis ve Lekkas, 2011). Bu durum bilginin güvenilirliğinin sağlanmasını önemli bir seviyeye taşımaktadır. Yönetim bilgi sisteminde,

var olan bilginin güvenliğinin sağlanması önemlidir ve bu duruma göre sistemsel koruma uygulamaları yer almaktadır.

### **2.3.2.Karar Destek Sistemleri**

Kurum içerisinde karar vermesine yardımcı olan bilgisayar tabanlı sistemdir. Karar destek sistemi, bilgilerin ve işlenmesinde kullanılan uygulamaların etkin bir şekilde kullanımı sağlanarak problemlerin karışmadan çözülmesine yardımcı olmaktadır. Sistem ile karar işlemleri yapılandırılır, planlama ve kontrol organizasyon çerçevesinde gerçekleştirilmesi sağlanır, kararlar otomatik şekilde verilmeye başlanır, bilgi taraması kolay bir şekilde yapılır, analitik temelde iş desteklenir.

Kurum içerisinde dört çeşit karar destek sistemi vardır. Bu sistemlerden biri veri besleme sistemidir. Öncesinde var olan bilgileri ve anlık raporları analiz etmekte kullanılmaktadır. Dosya çekme sistemi, veri analiz sistemi ve bilgi yürütme sistemi başlıkları altında incelenmektedir. Bir başka sistem olarak ele alınan tahmin sistemi, var olan durumun alternatif olarak değerlendirilen gelecek durumlara taşınması sistemidir. Tanımsal, nedensel ve olasılık sistemleri olarak değerlendirilmektedir. Tercih belirleme sistemi ise alternatif olarak var olan kararlar ile önceden alınmış olan kararlar arasında seçim yapmayı kolaylaştıran sistemdir. Karar ağacı ve çok özellikli karar sistemleri olarak ele alınmaktadır. Son sistem olarak ele alınan senaryo geliştirme sistemi ise analizden ayrı olarak karar vermede yaratıcılık unsurunu ön plana çıkartan sistemdir. Kavramaya ait planlama, fikir üretme, grup karar destek sistemleri olarak değerlendirilmektedir (Sönmez, 2014).

Karar destek sistemi, bilgiye kolay erişim sağlamasından dolayı bilginin güvenliğinin sağlanması noktasında kullanılacak ve aynı şekilde koruma sağlanması gerekli bir sistemdir. Kalite destek sisteminin gelişim süreci ve sistemin gelişim araçları, geliştiricinin deneyim ve yeterliliğine bağlı olarak donanımlaşmaktadır. Bu nedenle geliştiricinin, bilginin korunması noktasında gerekli bilgi ve beceriye sahip olması ve sistemdeki açığı tespit edip gerekli önlemlerin alınmasının sağlanmasını gerektirmektedir.

### 2.3.3. Veri, Veri Tabanı ve Veri Deposu

Veri, çözüm elde edebilmek için kullanılabilir duruma gelmiş bilgi ve bilgisayar için işlenebilir duruma getirilmiş sayısal ya da sayısal olmayan her türlü algı, ifade ve mesajdır. İnsan kaynakları yönetimince veri, çalışana ait tutulan özlük bilgilerin yer aldığı dosyaların her bir sayfasıdır. Amaç doğrultusunda veriler, işlenerek yöneticilerin kullanımına açılmış bir bilgi olarak ortaya çıkmaktadır. İnsan kaynakları işlevleri bünyesinde yer alan kadrolama başlığı altında incelenen seçme uygulamasında kurum, aranan pozisyon doğrultusunda gerekli yetkinliklere sahip insan kaynağını oluşturmak için oluşturduğu havuzda yer alan her bir özgeçmiş, bir veri olarak değerlendirilmektedir.

Veri tabanı ise kendi içerisinde sistematik düzeni olan ve bir başlık altında toplanabilen veriler bütünüdür. Veri tabanı, bilgiyi hızlı ve verimli bir şekilde yönetip değiştirebilmektedir, etkili kullanıldığı taktirde değer kazanmaktadır. Veri tabanlarının amacı, büyük miktardaki verilerin hızlı ve güvenli şekilde işlenerek ihtiyaç duyulan bilgiye dönüştürülmesidir ve dönüştürülen bilgiler düzenli bir şekilde elektronik ortama kaydedilirler. Bu şekilde çok sayıda uygulamanın ve kullanıcının erişimine sunulur. Veri tabanları, birçok kullanıcı tarafından kullanılan birbiriyle ilişkili geniş bir veri bütünü depoladığı için burada yetkili kişilerce istenilen veriye ulaşıyor olması önem taşımaktadır(Chen ve Chu, 2008).

Veri ambarı, farklı sistemlerden veriyi temin edip denetleyip değiştirdikten sonra anlaşılabilir ve kolay bir şekilde erişebilir hale getirir ve böylece geçmiş verileri depolar. Veri ambarına veriler giriş yapılmadan önce ETL veya ELT sürecinden geçmektedirler. ETL süreci, verinin kaynak sistemden alınması ile başlayarak verinin incelenmesi ve sisteme uygun olarak dönüştürülmesi olarak devam eder ve düzenlenmiş hali ile sisteme yüklenmesi yapılarak tamamlanır. ELT süreci ise verinin alınması ile başlayarak tek fark önce hedeflenen sisteme yüklenmesi yapıldıktan sonra istenilen forma dönüştürülmesi gerçekleşerek tamamlanmasıdır. Veri ambarında işlem yapılacak verilerin kaliteli olması önemlidir. Düzensiz veya üzerinde işlem yapmaya müsait olmayan veriler veri ambarında yanlış bilgilerin ortaya çıkmasına sebep olacaktır. Bu nedenle verilerin

işlenebilir oluşu, kalitesi önemli kriter olarak değerlendirilmektedir(Burtescu, 2009, ss.449-454 ).

### **2.3.4.İntranet, İnternet ve Kurumsal Bilgi Sistemleri**

İntranet, kurum içi ağ olarak açıklanabilmektedir. İnternetin kurum ihtiyaçlarına göre hazırlanmış ve verimli olarak idare edilip denetlenebilecek hale getirilmiş şeklidir de denilebilmektedir. Kurum bünyesinde var olan çalışanların birbirleriyle kesintisiz iletişim ve işbirliği halinde olmalarını sağlamaktadır. Çalışan, veri tabanlarına, raporlara ve yapmış oldukları işleri ile bilgilere tek bağlantıdan ulaşabilmektedir.

İnternet ise kişilerin birbirleri ile dünya üzerinde var olan bilgisayar ağlarının birleşiminden oluşan çok büyük bir bilgisayar ağıdır. Telefon hatları ile birbirine bağlı bu bilgisayar ağı, bünyesinde kişi ve kuruluşların kullanmış oldukları birbirinden farklı bilgisayarları ve bu bilgisayarlarda var olan farklı işletim sistemlerini barındırmaktadır. Birbirinden farklı bilgisayar ve işletim sistemlerinin ortak bir dille iletişim kurmasını sağlayarak kişilerin farklı programlar çalıştırsalar da ekranda aynı bilgileri görmelerini sağlamaktadır. İnternet, günümüzde teknolojinin de gelişmesiyle birlikte iletişim konusunda kullanılan önemli bir araç haline gelmiştir. Kullanımda ciddi kişi sayısına ulaşan internet, barındırdığı bilgilerin koruması noktasında da önemli bir kavram olarak ele alınması gerekli konuma gelmiştir. İnternet üzerinden gerçekleşen bilgi paylaşımları için şifrelemenin yapılarak bilgiye erişim izni olan kişinin bilgisinin korunması sağlanarak, virüs tarayıcılarının belli aralıklarla yapılarak veya virüslerin bilgisayarları zombi bilgisayara dönüştürerek üçüncü şahısların erişimini kolaylaştırmasının önüne geçilmesi için zararlı botnet yazılımlarını ortadan kaldırıp bilgiyi güvenlik altına alarak güvenlik zafiyetinin önüne geçilebilmektedir(Montesino, Fenz ve Baluja, 2012, ss.248-263). Bu gibi durumlar internetin güvenliği, internetin bilinçli kullanımı, internetin etik kullanımı, internet kullanıcılarının hukuki sorumluluklarının bilincinde olması gibi kavramlar önemli hale getirmiştir.

İnsan, donanım, yazılım, veri ve ağlar, kurumsal bilgi sistemi unsurları olarak değerlendirilirler. Bilgi sisteminin başarısını ölçen insandır. İnsan, sistemin kullanıcısıdır. Bu demektir ki sisteme giriş ve çıkışları gerçekleştiren, bunun için gerekli donanımları kullanabilen, program ve prosedürleri kuran, sisteme veri girişini sağlayan, ağ iletişimini gerçekleştiren insan unsurudur. Bu anlamda bir kurumda var olan bilgi sistemleri için çalışanlar önem taşımaktadır. Bununla birlikte değerlendirilecek olan diğer unsurlar bir bütün oluşturarak kurumlarda faaliyetlere, çalışan verimliliğine, müşteri memnuniyetine katkı sağlar, kurum yöneticilerine karar alım noktasında destek olur, ürün ve hizmetlerin geliştirilmesine sebep olur ve kurumların altyapılarını, kaynaklarını güçlendirmelerini sağlar. Verilerin girişinin yapılması ile oluşan kurumların bilgi sistemi, verilerin sınıflandırılarak sıralanması ve bilgi olarak işlenmesi ile geliştirilerek bilgi türlerini ortaya çıkartır ve bilgilerin kullanıma kadar korunmasını sağlayarak işlemeye devam eder. Giriş, süreç ve çıktı faaliyetlerinde veri ve bilgilerin korunması noktası büyük bir önem taşımaktadır. Bu anlamda kullanılan bilgi teknolojisi ile ortaya çıkan uygulamalar, bilgi sisteminde var olan çalışanların kurumsal sorumlulukları, bilginin kullanımı ve bilginin doğru bir şekilde yönetilmesi için izlenen stratejiler oluşabilecek güvenlik zafiyeti için değerlendirilen önemli başlıklar olarak karşımıza çıkmaktadır. Bilgi güvenliğini tehdit eden içsel ve dışsal unsurların bilgi sistemlerinden uzak durması için yapılan bilgi yedeklemeleri, virüs temizleme programları, güvenlik duvarı oluşturma, denetimli erişimin sağlanması gibi uygulamalar ile güvenlik zafiyetinin önüne geçilebilmektedir. Bilgi sistemlerinin önemli bir unsuru olarak değerlendirilen insan unsuru da bu anlamda üzerine düşen sorumluluğun farkında olarak bilinçli hareket edip bilgi güvenliği uygulamalarını yerine getirmelidir.

#### **2.4.Türkiye’de İnsan Kaynakları Yönetiminde Bilgi Güvenliği Uygulamaları Değerlendirilmesi**

Kurum bünyesinde oluşturulan bilgi güvenliği politikasına uygun olarak insan kaynakları yönetimi çalışanlarının iş süreçlerinde göz önünde bulundurulması gereken uygulamalar şu şekilde ele alınabilmektedir:

- ✓ Çalışanlar, bilgi güvenliği politikası doğrultusunda belirlenen uygulamaları iş süreçlerinde göz önünde bulundurmadıkları takdirde oluşan bilgi güvenliği zafiyetinden sorumludur.
- ✓ Çalışanlar işe giriş sürecinde gizlilik sözleşmesi imzalamalıdır.
- ✓ Çalışanlar işe giriş sürecinde kuruma ait bilgi güvenliği politikası maddelerinin yer aldığı ve iş süreçlerini göz önünde bulundurarak uyacağını taahhüt edeceği yazılı bir belge imzalamalı, çalışana konu ile ilgili olarak sözlü bilgilendirmede bulunmalıdır.
- ✓ Çalışanlara bilgi güvenliği uygulamaları farkındalık eğitimleri verilmelidir. Bu eğitimler yıl içerisinde belirli periyotlarla çalışana verileceği gibi her yeni işe başlayan çalışan için de işe başlangıç sürecinde verilebilmelidir.
- ✓ Kritik insan kaynakları yönetimi çalışmalarını bünyesinde barındıran bilgi teknoloji araçları, fiziksel erişim kontrol yetkisi bulunan insan kaynakları çalışanları veya yöneticilerinin erişebileceği alanlarda yer almalıdır.
- ✓ Sistem Odası Güvenlik Prosedürü'ne uygun olarak giriş yetkisi olmayan çalışanlar, çalışma alanında bulunmamalıdır.
- ✓ Özel izin alınmadığı takdirde çalışanların çalışma alanlarında iş süreleri içerisinde fotoğraf çekimi, ses kaydetmesi yasak olmalıdır.
- ✓ Güvenli alanlara giriş çıkış gerçekleşirken ziyaretçi defteri doldurulmalı, isim ve saatler kayıt altına alınmalıdır.
- ✓ Bilgi teknoloji araçlarından sorumlu çalışanların, herhangi bir elektrik kesintisinde bilgi teknoloji araçlarının çalışmalarına devam etmesi için kullanılan jeneratör gibi güç kaynağı yılda en az iki defa olmak üzere üretici kurum tarafından kontrolleri yaptırılmalıdır.
- ✓ Dizüstü bilgisayar, masa üstü bilgisayar, belge, taşınabilir bellek gibi bilgi donanımı açısından önemli varlıkların korunması için çalışanlar yetkilendirilmelidir.
- ✓ İnsan kaynakları çalışanları kayıtlı taşınabilir cihazlarını kurum dışına çıkardıklarında güvenlik prosedürü dahilinde hareket etmeli, bilgi işlem ve insan kaynakları yöneticisine yazılı/sözlü olarak bildirimde bulunmalıdır.

- ✓ İnsan kaynakları çalışanına ait şahsi taşınabilir cihazlar ile kuruma girilmesi yetkili izini ile mümkün olmalıdır.
- ✓ Hassas bilgiler içeren depolama cihazları ‘Hassas Ortam ve Teçhizat İmha Talimatı’ na göre işlenmelidir.
- ✓ İnsan kaynakları çalışanlarının, kullanmadıkları zamanlarda ekranlarının kilitleme özelliğini kullanarak yetkisi olmayan kişilerce görülmesini engellemelidir.
- ✓ İnsan kaynakları çalışanları kendilerine verilmiş olan kullanıcı ad ve şifrelerini kimseyle paylaşmamalıdır.
- ✓ Hassas bilgi içeren dokümanlara, yetkisi olmayan kişilerin erişimini engellemek için çalışanlar tarafından temiz masa politikası uygulanmalıdır. Önemli dokümanlar böylece kullanılmayan zamanlarda masa üstünden alınıp çekmecelere kaldırılmalıdır.
- ✓ İnsan kaynakları çalışanları, kullanmış oldukları masa çekmecelerini kilitli tutmalıdır.
- ✓ Kurum içi donanımların ve uygulamaların işletim prosedürlerine çalışanlar, ihtiyaç anında sürekli bir şekilde erişilebilen web, basılı ortamlardan ulaşabilmelidir.
- ✓ Olay yönetim prosedürleri belirlenerek güvenlik olayı başlangıcında, sırasında veya sonrasında yapılması gereken adımlar belirlenmeli ve yazılı/sözlü olarak çalışanlar ile paylaşılmalıdır.
- ✓ Bilgi güvenliği zafiyeti gerçekleştiğinde düzeltici önleyici faaliyet formu oluşturulmalı ve yardım masasına kaydı yapılmalıdır. Böylece eksiklikler belirlenerek tamamlanmalı ve zafiyetin önüne geçebilecek adımlar atılmalıdır. Taşınabilir ortamdaki bir bilgi artık kullanılmayacaksa çalışanlar tarafından silinmelidir.
- ✓ Bilgiler yetkisiz kişilerce paylaşılmamalıdır.
- ✓ İşlemler, prosedürler, veri yapıları gibi hassas bilgilerin bulunduğu sistem dokümantasyonu, yetkisi olmayan kişilerin erişimini engellemek için güvenli

ortamlarda bulundurulmalı, elektronik kopyalara iç ağ üzerinden yetkili kişilerin erişebileceği şekilde ulaşılabilir olmalıdır.

- ✓ Bilginin dağıtımı, nakli gibi durumlarda özel güvenli paketleme, güvenli kurye; elektronik ortam için sayısal imzalama veya şifreleme kullanılmalıdır.
- ✓ E-posta güvenliğinin sağlanması amacıyla Varlıkların Kullanımı Talimatı oluşturularak çalışanlar yazılı/sözlü olarak bilgilendirilmelidir.
- ✓ Erişim Kontrol ve Ağ Hizmetleri Kullanım Talimatı oluşturularak bilgilere erişim sağlanmalı ve talimattan çalışanlar yazılı/sözlü olarak bilgilendirilmelidir.
- ✓ Çalışanlar kendi hesaplarının şifrelerini paylaşmamalı, çalışma masalarından kalktıklarında elektronik cihazlarının oturumunu kilitlemelidir.
- ✓ İş sürekliliği planı oluşturularak olası iş akışını engelleyen durum yaşandığında insan kaynakları fonksiyonlarının aksamasının, bilgi kaybı yaşanmasının, izinsiz bilgi paylaşımının önüne geçilmelidir. İş sürekliliği planı ayda bir gerçekleşecek toplantı ile gözden geçirilmelidir.
- ✓ Çalışanlar, bilgi güvenlik ikaz ve ihlalleri, oluşturulan Bilgi Güvenliği İhlal Olay Bildirimi ve Yönetim Talimatı'na göre hareket ederek yetkiliye raporlamalıdır.
- ✓ Çalışanların kurum bilgi sistemi içerisinde var olan herhangi bir bilgiyi USB bellek, CD gibi ortamlara aktarması yasaktır. Bu duruma gerek olduğu durumlarda ise yetkiliden izin alınmalıdır.
- ✓ İnsan kaynakları çalışanı sorumluluğu altında bulunan veya şahsına ait olan diz üstü - masa üstü bilgisayardan, mobil cihazdan fotoğraf, doküman, belge paylaşmamalıdır.
- ✓ Kullanıcı bilgi güvenliği eğitimi çalışanlara verilmelidir.
- ✓ Çalışanlar, kullanıcı kimliklerini çalışma saatleri içinde iş gerekliliğine uygun bir şekilde kullanmalıdır.
- ✓ Bir daha kullanılmayacak veya ortadan kaldırılacak dokümanların evrak imha uygulamalarına uygun bir şekilde imha edilmesi gerekmektedir.

Çalışanlar, bahsedilmiş olan bilgi güvenliği uygulamalarını iş süreçlerinde göz önünde bulundurarak hareket ettiği taktirde bilgilerin daha güvenli bir şekilde sistemde



yer alması, paylaşılması gerekleşmiş ve bilgi güvenliđi zafiyetinin önüne geçilmiş olacaktır.

## BÖLÜM III

### 3.Yöntem

#### 3.1.1.Araştırma Amacı

Tezin amacı, Türkiye’de son zamanlarda teknolojinin gelişim ve değişimini hayatımıza çok daha kolay adapte edebiliyor ve toplum olarak ‘bilgi toplumu’ bilincini benimsemeye başlayırken karşımıza çıkan ‘bilgi güvenliği’ kavramının, iş hayatının önemli bir parçası haline gelmiş olan İnsan Kaynakları kavramı ile ne kadar ilişkili olduğunu ortaya koymaktadır.

#### 3.1.2.Araştırma Önemi

Tezin önemi, Türkiye’de bilgi güvenliği uygulamalarının insan kaynakları çalışanları ve yöneticileri tarafından dikkate alınarak var olan iş süreçlerinde göz önünde bulundurularak bilgi güvenliği zafiyetinin önüne geçilmesi konusunda farkındalık yaratabilmektir.

#### 3.1.3.Araştırma Yöntemi

Nicel yöntemlerden biri olan betimsel yöntem ile yazılmış olan bu tez çalışması, araştırma amacı, araştırma önemi, araştırma yöntemi, araştırma problemi, evren ve örneklem, veri toplama araçları açısından değerlendirilirken, veri analizi noktasında kullanılan istatistiksel tekniklerin uygunluğu ile detaylı bir inceleme yapılarak hazırlanmıştır. IBM SPSS Statistics 23 yazılımı kullanılarak 413 çalışanın verdiği cevaplar aktarılmış ve istatistiksel analizi yapılmıştır. İş süreçlerinde bilgi güvenliği uygulamaları ile görüşlerin oluşturduğu anket, açımlayıcı faktör analizi ile incelenmiştir. Açımlayıcı faktör analizi uygulanırken yöntem olarak “Temel Bileşenler Analizi” ve döndürme olarak “Varimax”tan faydalanılmıştır. Oluşan yapıların iç tutarlılığını ölçmek için Cronbach Alfa güvenilirlik katsayısı yorumlanmıştır.

### **3.1.4.Araştırma Problemi**

Bu tez çalışması ile Türkiye’de insan kaynakları yönetiminde bilgi güvenliği uygulamalarına, insan kaynakları çalışanları ve yöneticileri tarafından ne ölçüde dikkat edilerek iş süreçlerinin devamlılığı sağlanıyor sorusuna cevap bulunmak istenmiştir.

### **3.1.5.Araştırma Hipotezi**

Tez çalışması hipotezi, Türkiye’de insan kaynakları yönetiminde, insan kaynakları çalışanları ve yöneticileri tarafından bilgi güvenliği uygulamalarının, iş süreçlerinin devamlılığında yansıtılmamaktadır.

### **3.1.6.Evren ve Örneklem**

Araştırma evrenini, Türkiye’de bilişim teknolojileri, eğitim, enerji, gıda, inşaat, medya-iletişim-yayıncılık ve turizm sektörlerinde faaliyet gösteren 72 kurum oluşturmaktadır. Bu kurumların insan kaynakları çalışanı ve yöneticilerinden oluşmak üzere toplam 413 çalışan ise araştırmanın örneklemini oluşturmaktadır.

### **3.1.7.Veri Toplama Araçları**

Türkiye’de insan kaynakları yönetiminin var olduğu kurumların tespit edilmesi, bilgi güvenliği politikalarının incelenmesi ve bu doğrultuda insan kaynakları yönetimi süreçlerinde bilgi güvenliği uygulamalarının hangi ölçüde göz önünde bulundurularak iş süreçlerinin devamlılığının sağlandığının tespiti, analizi ve değerlendirilmesi amacıyla Türkiye’de faaliyet gösteren 72 kurumun toplam 413 insan kaynakları çalışanı ve yöneticisi ile yüz yüze görüşülmüş ve birebir anket yapılarak araştırma değerlendirilmiştir. İş süreçlerinde göz önünde bulundurulmuş/bulundurulmamış olan bilgi güvenliği politikaları uygulamaları yerinde, zamanında gözlemlenmiş ve bu doğrultuda değerlendirme ölçeği belirlenmiştir. 5’li likert 38 maddeden oluşan, bilgi güvenliği politikası baz alınarak hazırlanmış, 3 başlık altında değerlendirilmeye alınmış olunan, kurumların bilgi güvenliği politikaları doğrultusunda oluşmuş olan bilgi

güvenliği uygulamaları baz alınarak oluşturulmuş anket ile tez çalışma değerlendirilmesi yapılmıştır.

İnsan kaynakları yönetimi ve bilgi teknolojileri ile ilgili 13'ü web site, 35'i kitap/dergi/makale yayını olmak üzere toplam 49 kaynaktan ön araştırma yapılarak yararlanılmıştır.

### **3.1.8.Verilerin Analizi ve Güvenilirlik**

Türkiye'de insan kaynakları yönetimi var olan 72 kurumun insan kaynakları yönetim süreçlerinde bilgi güvenliği politika uygulamaları, insan kaynakları çalışanı ve yöneticilerinden alınan nicel verilerin değerlendirme ölçeği doğrultusunda betimleyici istatistikler kullanılarak yorumlanmıştır.

Çalışmada elde edilen bulgular değerlendirilirken, istatistiksel analizler için SPSS 23.0 İstatistik paket programı kullanılmıştır. Çalışma verileri değerlendirilirken tanımlayıcı istatistiksel metotları (Frekans, Yüzde, Ortalama, Standart sapma) yönteminden faydalanılmıştır.

Niceliksel verilerin karşılaştırılmasında iki grup durumunda, normal dağılım gösteren parametrelerin gruplar arası karşılaştırmalarında Bağımsız örnekler (Independent samples) t testi, niceliksel verilerin karşılaştırılmasında ikiden fazla grup durumunda, normal dağılım gösteren parametrelerin gruplar arası karşılaştırmalarında Tek yönlü (One way) Anova testi ve farklılığa neden olan grubun tespitinde Tukey testi kullanılmıştır. Sonuçlar % 95 güven aralığında,  $p < 0,05$  anlamlılık düzeyinde değerlendirilmiştir.

Araştırmada elde edilen verilerin güvenilirliklerinin test edilmesi için yapılan Cronbach's Alpha testi neticesinde ölçekte yer alan verilerin Cronbach's Alpta test istatistiği 0,818 olduğu sonucuna varılmıştır. Bu sonuç verilerin güvenilir olduğunu göstermektedir.

### 3.2.Bulgular

#### 3.2.1.Faktör Analizine Yönelik Bulgular

Araştırmada kullanılan ve araştırmacı tarafından hazırlanan ölçeğin geçerliliği ve ölçek boyutları faktör analizi ile incelenmiştir. Ölçeğin faktör analizine uygunluğunun test edilmesi için gerçekleştirilen KMO-Barlett Küresellik testi sonuçlarına göre ise KMO test istatistiğinin 0,822 düzeyinde ve Bartlett Küresellik testinin 0,00 anlamlılık seviyesinde olduğu ve ölçeğin faktör analizine uygun olduğu sonucu elde edilmiştir.

**Tablo 2.** Faktör Analizi

Madde	Boyutlar			Açıklanan Varyans
	Güvenlik	Süreç	Bildirim	
1	,745			34,22
2	,618			
3	,684			
4	,759			
5	,622			
6	,824			
7	,603			
8	,802			
9	,791			
10	,734			
11	,667			
12	,691			
13	,704			
14	,746			
15	,691			
16	,752			
17	,694			
18	,778			
19	,691			
20	,672			
21		,891		48,67
22		,773		
23		,748		
24		,693		
25		,608		
26			,587	69,44

27			,671
28			,594
29			,671
30			,703
31			,794
32			,608
33			,653
34			,681
35			,642
36			,673
Toplam Açıklanan Varyans			69,44

Araştırmada, insan kaynakları yönetimi uygulamalarında bilgi güvenliği uygulamalarının araştırıldığı ölçeğin faktör yapılarına bakıldığında ölçeğin toplam varyansının %69,44'ünü açıklar düzeyde 3 faktörde incelenebileceği görülmüştür. Bu faktörler, Güvenlik (20 Madde), Süreç (5 Madde) ve Bildirim (11 Madde) faktörleridir.

### 3.2.2. Demografik Özelliklere İlişkin Bulgular

**Tablo 3.** Cinsiyete Göre Dağılım

		Frekans	Yüzde	Geçerli Yüzde	Kümülatif Yüzde
	Kadın	218	52,8	52,8	52,8
	Erkek	195	47,2	47,2	100,0
	Total	413	100,0	100,0	

Araştırmaya dahil olan katılımcılar cinsiyetlerine göre %52,8 (218 Kişi) Kadın, %47,2 (195 Kişi) Erkek şeklinde dağılmıştır.

**Tablo 4. Yaşa Göre Dağılım**

	Frekans	Yüzde	Geçerli Yüzde	Kümülatif Yüzde
24-35 Yaş	68	16,5	16,5	16,5
36-45 Yaş	181	43,8	43,8	60,3
46-55 Yaş	132	32,0	32,0	92,3
56 Yaş ve Üstü	32	7,7	7,7	100,0
Total	413	100,0	100,0	

Araştırmaya dahil olan katılımcılar yaşlarına göre %43,8 (36-45 Yaş), %32 (132 Kişi) 46-55 Yaş, %16,5 (68 Kişi) 24-35 Yaş ve %7,7 (32 Kişi) 56 yaş ve üstü şeklinde dağılmıştır.

**Tablo 5. Eğitim Durumuna Göre Dağılım**

	Frekans	Yüzde	Geçerli Yüzde	Kümülatif Yüzde
İlköğretim	10	2,4	2,4	2,4
Lise ve Dengi	40	9,7	9,7	12,1
Önlisans	131	31,7	31,7	43,8
Lisans	184	44,6	44,6	88,4
Yüksek Lisans	39	9,4	9,4	97,8
Doktora	9	2,2	2,2	100,0
Total	413	100,0	100,0	

Araştırmaya dahil olan katılımcılar eğitim durumlarına göre %44,6 (184 Kişi) Lisans, %31,7 (131 Kişi) Önlisans, %9,7 (40 Kişi) Lise ve Dengi, %9,4 (39 Kişi) Yüksek Lisans, %2,4 (10 Kişi) İlköğretim ve %2,2 (9 Kişi) Doktora şeklinde dağılmıştır.

**Tablo 6. Medeni Duruma Göre Dağılım**

	Frekans	Yüzde	Geçerli Yüzde	Kümülatif Yüzde
Evli	250	60,5	60,5	60,5
Bekar	163	39,5	39,5	100,0
Total	413	100,0	100,0	

Araştırmaya dahil olan katılımcılar medeni durumlarına göre %60,5 (250 Kişi) Evli, %39,5 (163 Kişi) Bekar şeklinde dağılmıştır.

**Tablo 7. Mesleklerine Göre Dağılım**

		Frekans	Yüzde	Geçerli Yüzde	Kümülatif Yüzde
	İnsan Kaynakları Birimi Çalışanı	280	67,8	67,8	67,8
	İnsan Kaynakları Birimi Yöneticisi	133	32,2	32,2	100,0
Total		413	100,0	100,0	

Araştırmaya dahil olan katılımcılar mesleklerine göre %67,8 (280 Kişi) insan kaynakları birimi çalışanı, %32,2 (133 Kişi) insan kaynakları birimi yöneticisi şeklinde dağılmıştır.

### 3.2.3.Araştırmanın Hipotezine İlişkin Bulgular

**Tablo 8. Katılımcıların İnsan Kaynakları Yönetiminde Bilgi Güvenliği Uygulamalarına Yönelik Belirttikleri Görüşlerin Cinsiyetlerine Göre Farklılık Analizi**

	Cinsiyet	N	Ort.	Std. Sapma	F	Sig.p.
Güvenlik	Kadın	218	2,8456	,21795	1,221	0,781
	Erkek	195	2,8518	,23167		
Süreç	Kadın	218	2,6550	,40172	2,938	0,800
	Erkek	195	2,6656	,44652		
Bildirim	Kadın	218	2,9428	,29110	0,278	0,722
	Erkek	195	2,9531	,29069		

Araştırmaya dahil olan katılımcıların insan kaynakları yönetiminde bilgi güvenliği uygulamalarına yönelik belirttikleri görüşlerin cinsiyetlerine göre farklılık analizi Bağımsız T – Testi ile incelenmiştir. Analiz neticesinde katılımcıların insan kaynakları yönetiminde bilgi güvenliği uygulamalarına yönelik belirttikleri görüşlerin cinsiyetlerine göre farklılık göstermediği tespit edilmiştir (Sig.p. > 0,05).



**Tablo 9.** Katılımcıların İnsan Kaynakları Yönetiminde Bilgi Güvenliği Uygulamalarına Yönelik Belirttikleri Görüşlerin Yaşlarına Göre Farklılık Analizi

		N	Ort.	Std. Sapma	F	Sig.p.
Güvenlik	24-35 Yaş	68	2,8544	,23352	0,584	0,626
	36-45 Yaş	181	2,8392	,21057		
	46-55 Yaş	132	2,8470	,24337		
	56 Yaş ve Üstü	32	2,8953	,20014		
	Total	413	2,8485	,22428		
Süreç	24-35 Yaş	68	2,6324	,48205	0,133	0,940
	36-45 Yaş	181	2,6685	,41760		
	46-55 Yaş	132	2,6652	,38084		
	56 Yaş ve Üstü	32	2,6500	,49774		
	Total	413	2,6600	,42298		
Bildirim	24-35 Yaş	68	2,9457	,25254	0,635	0,593
	36-45 Yaş	181	2,9388	,31317		
	46-55 Yaş	132	2,9720	,27437		
	56 Yaş ve Üstü	32	2,9014	,30284		
	Total	413	2,9477	,29060		

Araştırmaya dahil olan katılımcıların insan kaynakları yönetiminde bilgi güvenliği uygulamalarına yönelik belirttikleri görüşlerin yaşlarına göre farklılık analizi Tek Yönlü ANOVA Testi ile incelenmiştir. Analiz neticesinde katılımcıların insan kaynakları yönetiminde bilgi güvenliği uygulamalarına yönelik belirttikleri görüşlerin yaşlarına göre farklılık göstermediği tespit edilmiştir (Sig.p. > 0,05).

**Tablo 10.** Katılımcıların İnsan Kaynakları Yönetiminde Bilgi Güvenliği Uygulamalarına Yönelik Belirttikleri Görüşlerin Eğitim Durumlarına Göre Farklılık Analizi

		<b>N</b>	<b>Ort.</b>	<b>Std. Sapma</b>	<b>F</b>	<b>Sig.p.</b>
Güvenlik	İlköğretim	10	2,8200	,20303	1,007	0,413
	Lise ve Dengi	40	2,8650	,26942		
	Önlisans	131	2,8485	,23525		
	Lisans	184	2,8313	,20892		
	Yüksek Lisans	39	2,9154	,20169		
	Doktora	9	2,8722	,25994		
	Total	413	2,8485	,22428		
Süreç	İlköğretim	10	2,6400	,41952	0,995	0,420
	Lise ve Dengi	40	2,5550	,42120		
	Önlisans	131	2,6748	,43701		
	Lisans	184	2,6793	,40219		
	Yüksek Lisans	39	2,6769	,44631		
	Doktora	9	2,4667	,53852		
	Total	413	2,6600	,42298		
Bildirim	İlköğretim	10	2,8077	,27676	1,404	0,222
	Lise ve Dengi	40	2,9038	,27474		
	Önlisans	131	2,9383	,30657		
	Lisans	184	2,9523	,28027		
	Yüksek Lisans	39	3,0355	,27387		
	Doktora	9	2,9573	,37510		
	Total	413	2,9477	,29060		

Araştırmaya dahil olan katılımcıların insan kaynakları yönetiminde bilgi güvenliği uygulamalarına yönelik belirttikleri görüşlerin eğitim durumlarına göre farklılık analizi Tek Yönlü ANOVA Testi ile incelenmiştir. Analiz neticesinde katılımcıların insan kaynakları yönetiminde bilgi güvenliği uygulamalarına yönelik belirttikleri görüşlerin eğitim durumlarına göre farklılık göstermediği tespit edilmiştir (Sig.p. > 0,05).

**Tablo 11.** Katılımcıların İnsan Kaynakları Yönetiminde Bilgi Güvenliği Uygulamalarına Yönelik Belirttikleri Görüşlerin Medeni Durumlarına Göre Farklılık Analizi

	Medeni	N	Ort.	Std. Sapma	F	Sig.p.
Güvenlik	Evli	250	2,8670	,22459	0,150	<b>0,038</b>
	Bekar	163	2,8202	,22150		
Süreç	Evli	250	2,6584	,39752	3,773	0,922
	Bekar	163	2,6626	,46055		
Bildirim	Evli	250	2,9338	,28467	0,235	0,232
	Bekar	163	2,9689	,29910		

Araştırmaya dahil olan katılımcıların insan kaynakları yönetiminde bilgi güvenliği uygulamalarına yönelik belirttikleri görüşlerin medeni durumlarına göre farklılık analizi Bağımsız T – Testi ile incelenmiştir. Analiz neticesinde evli katılımcıların insan kaynakları yönetiminde bilgi güvenliği uygulamalarına yönelik görüşlere katılım düzeylerinin bekar katılımcılara göre daha yüksek düzeyde olduğu tespit edilmiştir (Sig.p. < 0,05).

**Tablo 12.** Katılımcıların İnsan Kaynakları Yönetiminde Bilgi Güvenliği Uygulamalarına Yönelik Belirttikleri Görüşlerin Mesleklerine Göre Farklılık Analizi

	Meslek	N	Ort.	Std. Sapma	F	Sig.p.
Güvenlik	İnsan Kaynakları Birimi Çalışanı	280	2,8464	,22217	0,001	0,783
	İnsan Kaynakları Birimi Yöneticisi	133	2,8530	,22944		
Süreç	İnsan Kaynakları Birimi Çalışanı	280	2,6729	,43318	1,117	0,360
	İnsan Kaynakları Birimi Yöneticisi	133	2,6331	,40089		
Bildirim	İnsan Kaynakları Birimi Çalışanı	280	2,9552	,30087	1,479	0,444
	İnsan Kaynakları Birimi Yöneticisi	133	2,9318	,26809		

Araştırmaya dahil olan katılımcıların insan kaynakları yönetiminde bilgi güvenliği uygulamalarına yönelik belirttikleri görüşlerin mesleklerine göre farklılık analizi Bağımsız T – Testi ile incelenmiştir. Analiz neticesinde katılımcıların insan kaynakları yönetiminde bilgi güvenliği uygulamalarına yönelik belirttikleri görüşlerin mesleklerine göre farklılık göstermediği tespit edilmiştir (Sig.p. > 0,05).

**Tablo 13.** Bilgi Güvenliği Uygulamaları Düzeyleri

Descriptive Statistics			
	N	Mean	Std. Deviation
Güvenlik	413	2,8485	,22428
Süreç	413	2,6600	,42298
Bildirim	413	2,9477	,29060
Valid N (listwise)	413		

Katılımcıların insan kaynakları yönetiminde bilgi güvenliği uygulamalarına yönelik görüşlerinin düzeylerine bakıldığında bilgi güvenliği uygulamaları bildirim ile ilgili görüşlere diğer görüşlerden daha yüksek düzeyde katıldıkları görülmektedir.

Katılımcıların en düşük düzeyde ise bilgi güvenliđi uygulamalarının süreç ile ilgili olan görüşlerine en düşük düzeyde katıldıkları görölmüştür.

## SONUÇ VE ÖNERİLER

Türkiye’de kamu ve özel sektörde faaliyet gösteren kurumların insan kaynakları çalışanları ve yöneticileri ile yapılmış olan anket doğrultusunda elde edilmiş olan veriler, yapılan incelemeler göstermektedir ki bilgi güvenliği politikası bilinci, çalışanlarda ve yöneticilerde teorik anlamda yer almakta fakat bilgi güvenliği uygulamalarının göz önünde bulundurularak iş süreçleri yönetilememektedir. Anket sorularının değerlendirilmesiyle tespit edilmiştir ki iş süreçlerinde ‘sıklıkla’ bilgi güvenliği politikalarına uygun hareket eden çalışanların %83,9 oranının, ‘genellikle’ cevabını veren çalışanların %88,1 oranının lisans mezunu olduğu tespit edilmiştir. Bu anlamda iş süreçlerinde bilgi güvenliği uygulamalarının göz önünde bulundurulması adına çalışanlarda farkındalık yaratmak eğitim ile mümkün olabileceği tespit edilmiştir.

Araştırmada gerçekleştirilmiş olan anket çalışmasına katılım sağlayan 143 çalışanın %52,8’i (218 Kişi) Kadın, %47,2 (195 Kişi) Erkek çalışandan oluşmaktadır. Bu dağılımın araştırma sırasında homojen dağılması önemsenmiştir.

Araştırmaya katılan çalışanların %43,8’i (181 Kişi) 36-45 Yaş, %32 (132 Kişi) 46-55 Yaş, %16,5 (68 Kişi) 24-35 Yaş ve %7,7 (32 Kişi) 56 yaş ve üstü şeklinde dağılmıştır. Bununla birlikte çalışanların eğitim durumlarına göre %44,6 (184 Kişi), %31,7 (131 Kişi), %9,7 (40 Kişi) Lise ve Dengi, %9,4 (39 Kişi) %2,4 (10 Kişi) İlköğretim ve %2,2 (9 Kişi) Doktora şeklinde dağılmıştır. Çalışanların %60,5’i (250 Kişi) Evli, %39,5’i ise (163 Kişi) Bekar şeklinde dağılmıştır.

Araştırmada çalışanların insan kaynakları yönetiminde bilgi güvenliği uygulamalarının demografik özelliklere göre farklılıkları incelenmiştir. Elde edilen sonuçlara bakıldığında çalışanların insan kaynakları yönetiminde bilgi güvenliği uygulamalarının medeni durumlarına göre farklılık gösterdiği görülmüştür. Elde edilen sonuçlar evli çalışanların bilgi güvenliği uygulamalarının ‘güvenliğe’ ilişkin görüşlerine katılım düzeyleri, bekar çalışanların katılım düzeyine göre daha yüksek olduğu tespit edilmiştir. Bu durum evli çalışanların insan kaynakları yönetimi süreçlerinde bilgi

güvenliği uygulamalarını göz önünde bulundurulduğunda ‘güvenlik’ ile ilgili yeterliliklerin yerine gelmesine yönelik görüşlere bakıldığında bekar çalışanlardan daha fazla katıldıkları ifade edilebilmektedir.

Genel olarak bilgi güvenliği uygulamalarının insan kaynakları yönetiminde uygulanma düzeylerine bakıldığında, bilgi güvenliği uygulamaları gereklerine büyük oranda önem verilmediği görülmektedir. Özellikle bilgi güvenliği uygulamalarının süreç boyutunun çalışanların en düşük düzeyde katılım gösterdiği görülmüştür.

Türkiye’de insan kaynakları yönetimi bünyesinde yer alarak faaliyet gösteren kurumların, bilgi güvenliği politikalarının var olduğu fakat uygulamada etkinlik sağlayamamış olduğu tespit edilmiştir. Bu anlamda Türkiye’de faaliyet gösteren kurumların, insan kaynakları yönetim süreç ve uygulamalarının denetimi sağlanarak, insan kaynakları süreçlerinde bilgi güvenliği politika modeli oluşturulmalı ve sürecin takibi sağlanmalıdır. Bu model ile ilk olarak güvenlik politikasının uygulama alanları belirlenmelidir. Tespitler doğrultusunda, bilgi güvenliği yönetim sistem ekibi oluşturularak uygulamaya geçecek faaliyetler ortaya konulmalıdır. ISO 27001 Bilgi Güvenliği Standartları doğrultusunda ortaya konulan faaliyet ve uygulamalar hakkında çalışanlar yazılı/sözlü olarak bilgilendirilmeli, kurum yöneticilerinin senede bir kez çalışanlar ile birlikte bilgi güvenliği politika işleyişi hakkında görüşme yapmaları sağlanmalı, zaafiyet ve eksiklikler gözden geçirilip değerlendirilmeli, bu doğrultuda alınacak olan eylemler belirlenmelidir. Kurum dışı ve kurum içi sisteme erişim durumunda hangi uygulamalar göz önünde bulundurulmalı, nasıl bir prosedür izlenmeli, güvenlik zaafiyetinin nasıl önüne geçilmeli hususları doğrultusunda işleyiş belirlenmelidir.

Şu an üzerinde çalışılmakta olan bir yazılım ve algoritması ile Bilgi Teknolojileri ve Kişisel Verilerin Korunması Kurumları tarafından ortak bir sistem oluşturulmuş olarak sistem dahilinde yer alan kurumların en azından sistemsel olarak bilgi güvenlik politikasına uygun hareket edip etmedikleri tespit edilebilir olabilecektir. Üzerinde çalışılan bu yazılım ile kurumlar, bilgi güvenliği zaafiyeti konusunda kontrol ve denetim altına alınmış olacaktır.

## KAYNAKÇA

- Accenture. (2018). December 2018 Tarihinde *Cyber Thearscape Report*:  
[https://www.accenture.com/\\_acnmedia/PDF-83/Accenture-Cyber-Threatscape-Report-2018.pdf#zoom=50](https://www.accenture.com/_acnmedia/PDF-83/Accenture-Cyber-Threatscape-Report-2018.pdf#zoom=50) adresinden alındı
- Aldemir, C., Ataol, A., & Budak, G. (2001). *İnsan Kaynakları Yönetimi*. İzmir: Barış Yayınları.
- Aon. (2018) *Şirket Birleşmeleri ve Satın Almaları Raporu*.  
<https://www.fortuneturkey.com/riske-karsi-sigorta-sermayesi> adresinden alındı.
- Arbor. (2018). *Siber Tehdit Ortamı Araştırma Raporu*.  
<https://www.dunya.com/kose-yazisi/siber-saldirilarda-terabit-cagi-basladi/429323> adresinden alındı
- Arıcı, K. (1999) *İşçi Sağlığı ve İş Güvenliği Dersleri*, Ankara, Tes-İş Eğitim Yayınları, Ankara.
- Armstrong, M. (2000). *Strategic Human Resources Management: A Guide to Action*. London: Kogan Page.
- Aslan, O. E. (2012). *Maaş İlişkisi ve Türkiye'de Memur Maaşları: 1970-2008*. Amme İdaresi Dergisi, 44, 109-140.
- Bayraktaroğlu, S. (2006). *İnsan Kaynakları Yönetimi*. Ankara: Gazi Kitabevi.
- BGA Security. (2018). Haziran 2019 Tarihinde *Siber Tehdit İstihbaratı*:  
[www.bgasecurity.com/2018/01/siber-tehdit-istihbarati](http://www.bgasecurity.com/2018/01/siber-tehdit-istihbarati) adresinden alındı
- BSI. (2004) *Critical Infrastructure Protection: Survey of World-Wide Activities*, Federal Office for Information Security (BSI), 3-9.



- Burtescu, E. (2009) *Database Security-Attacks and Control Methods*. Journal of Applied Quantitative Methods, 449–454.
- Cabinet Office, “*A Strong Britain in an Age of Uncertainty: The National Security Strategy*”, 2010.
- Calder, A. (2009). *Information Security based on ISO 27001/ISO 27002-A Management Guide*. 12, 23-25 Van Heren Publishing.
- Chen, Y., Chu W. W. (2008) *Protection of Database Security via Collaborative Inference Detection*. Springer.
- Chene, M. (2009). *The Implementation of Integrated Financial Information Management Systems (IFMIS)*. Transparency International, 2(1).
- Cortada, James W. (1998) “*Best Practices in Information Technology*”, Prentice Hall, 1-68.
- Çevikbaş, R. (1995). *Türk Kamu Yönetiminde Personel Rejimi ve Uygulama Süreci*. Amme İdaresi Dergisi, 2, 51-80.
- Dunphy, D., Turner, D. ve Crawford, M. (1997) ‘Organizational Learning as the Creation of Corporate Competencies’, Journal of Management Development, 16 (4).
- Dülger, Ü. (2016). *Bilimsel Gelişme, Buluş ve Keşiflerin Ülkelere Göre Dağılımı*. Yeni Türkiye Dergisi, 365.
- Demirkaya, H. (2015). *Türkiye’de İnsan Kaynakları Yönetimi Anlayışındaki Dönüşümlerin Organizasyonlarındaki Yansımaların Araştırması*. İzmit: Umuttepe Yayınları.
- Erçek, M. (2004). *Aktör Ağları ve Eksik/Öncül Kurumsallaşma: Türkiye’deki Mesleki Personel/İnsan Kaynakları Söyleminin Yeniden Kurgulanması: 1960-1999*. Yönetim Araştırmaları Dergisi, 2, 129-195.

- Ersoy, E.V. (2012). *ISO/IEC 27001 Bilgi Güvenliđi Standardı*. ODTÜ Yayıncılık, Ankara.
- Esen, M. (2018, November 12). *Bilgi Güvenliđi Nedir ve Nasıl Sınıflandırılır?* Sibergah: <http://www.sibergah.com/genel/bilgi-guvenligi-nedir-ve-nasil-siniflandirilir> adresinden alındı.
- Grover, V., Fiedler, K. D. ve Teng, J. T. C., (1999). "*The role of organizational and information technology antecedents in reengineering initiation behaviour*" *Decision Sciences*, 30.
- Gürol, C., Sađırođlu, Ő. (2006) "*Bilgi, Bilgi Güvenliđi ve Süreçleri Üzerinde Bir İnceleme*" *Politeknik Dergisi*, 3, 165-174
- Güvenen, O., (1998) *Küreselleşme Sürecinde Bilgi Teknolojileri ve Bilgi Sistemleri Stratejileri*. DPT, Ön Çalışma Raporu, İstanbul.
- Güzel, A. (1986). *3008 Sayılı İş Yasasının Önemi ve Başlıca Hükümleri*. Sosyal ve Siyaset Konferansı Dergisi, 35-36.
- ISO/IEC 27001:2005. (2005). January 2019 tarihinde <https://www.iso.org/obp/ui/#iso:std:iso-iec:27001:ed-1:v1:en> adresinden alındı
- ISO/IEC 27001:2013. (2013). January 2019 tarihinde <https://www.iso.org/obp/ui/#iso:std:iso-iec:27001:ed-2:v1:en> . adresinden alındı
- Kişisel Verilerin Otomatikleşmeye Tabi Tutulması Karşısında Bireylerin Korunması Sözleşmesi. (1981, January 28). December 2018 tarihinde *Human Rights Center*: <https://humanrightscenter.bilgi.edu.tr/media/uploads/2016/03/29/KisiselVerilerinOtomatikIslemeTabiTutulmasiKarsisindaBireylerinKorunmasiSozlesmesi.pdf> adresinden alındı
- Maguire, S., Redman, T. (2007). *The Role of Human Resource Management in Information Systems Development*. *Management Decision*. 45(2): 252-264.

Montesino, R., Fenz S., Baluja W. (2012) *Siem-Based Framework for Security Controls Automation*. Information Management & Computer Security, 248–263.

Muhteşem, B. (2002). “*The New HR Practices in Changing Organizations: An Empirical Study in Turkey*”, Journal of European Industrial Training (26), 81-87.

National Information Security Policy Council, Japan. (2006) “Secure Japan 2006 - First Step toward a Trustworthy Society”.

[http://www.nisc.go.jp/eng/pdf/sj2006\\_eng.pdf](http://www.nisc.go.jp/eng/pdf/sj2006_eng.pdf) adresinden alındı.

National Institute Of Standards And Technology. (2004) “FISMA Overview”

<http://csrc.nist.gov/organizations/fissea/2004-conference/presentations/Thursday/Fabius-FISSEA-031104.ppt> adresinden alındı.

Mathis, R., Jacson, J. (2006). *Human Resources Management*. Thomson South Western, 44, 1-32.

Öktem, K. (1992). *Türk Kamu Personel Yönetiminin Gelişimi*. Amme İdaresi Dergisi, 29(2), 85-105.

Özdemir, M. (2014). *Eğitim Örgütlerinde İnsan Kaynakları Yönetimi*. Ankara: Anı Yayıncılık.

Recordo, R., Jolly, J. (1997). *Organizational Culture and Teams*. S.A. M. Advanced Management Journal. Vol. 62.

Society for Advancement of Management U. S. A

Sönmez, C. (2014). İstanbul Teknik Üniversitesi. 2019 tarihinde

<https://web.itu.edu.tr/~sonmez/lisans/es/KararDestek.pdf> adresinden alındı

STM. (2018) March 2018 Tarihinde *Siber Tehdit Durum Tespit Raporu*:

<https://www.stm.com.tr/tr/haberler/duyurular/siber-tehdit-durum-raporu-ocak-mart-2018> adresinden alındı

- Salih, G. (2012). *Örgütsel Davranış*. Ankara: Nobel Akademik Yayıncılık.
- Şen Ş., Yerlikaya T. (2013). *ISO 27001 Kurumsal Bilgi Güvenliği Standardı*.  
Akademik Bilişim 2013, Akdeniz Üniversitesi, Antalya, 23 - 25 Ocak 2013.
- Taymaz, H. (1981). *Hizmet İçi Eğitim: Kavramlar, İlkeler, Yöntemler*. Ankara: Ankara Üniversitesi, Eğitim Fakültesi Yayınları, Sevinç Matbaası.
- The World Bank. (2016) World Bank Open Data.  
<http://data.worldbank.org/> adresinden alındı.
- Tonta, Y.(1999) “*Bilgi Toplumu ve Bilgi Teknolojisi*” Türk Kütüphaneciliği, 13, 4.
- Yüksel, Ö.(1998). *İnsan Kaynakları Yönetimi*. Ankara: Gazi Kitabevi.
- Zissis, D., Lekkas, D. (2011). *Addressing Cloud Computing Security Issues*. Future Generation Computer Systems, In Press, Corrected Proof
- Westerlund, M., Leminen, S. and Rajahonka, M. (2014) *Designing Business Models for the Internet of Things*. Technology Innovation Management Review, 5.



## EK 1: Anket Formu

### TÜRKİYE'DE İNSAN KAYNAKLARI YÖNETİMİNDE BİLGİ GÜVENLİĞİ UYGULAMALARI

#### Sayın Katılımcı;

*İnsan kaynakları yönetimi süreçlerinde bilgi güvenliği politikası uygulamalarının etkinliğini ölçmeyi amaçlayan bu anket çalışmasını cevaplandırmak yaklaşık olarak 10 dakikanızı alacak olup bu çalışma, bilimsel amaçlı bir çalışmadır. **Verdiğiniz bilgiler kesinlikle bilimsel amaçlar dışında kullanılmayacak ve gizli tutulacaktır.** Lütfen soruları dikkatle okuyup size en uygun gelen cevabı işaretleyiniz. Katkılarınız ve anketi doldurmada gösterdiğiniz ilgi ve özen için teşekkür ederiz.*

Merve ÜNVER  
Atılım Üniversitesi Sosyal Bilimler Enstitüsü  
İşletme Tezli Yüksek Lisans

#### 1) Cinsiyetiniz:

- ( ) Kadın  
( ) Erkek

#### 2) Yaşınız:

- ( ) 24 – 35 yaş arası  
( ) 36 – 45 yaş arası  
( ) 46 – 55 yaş arası  
( ) 56 yaş ve üstü

#### 3) Eğitim Durumunuz:

- ( ) İlköğretim  
( ) Lise ve Dengi  
( ) Ön lisans  
( ) Lisans  
( ) Yüksek Lisans  
( ) Doktora

**4) Medeni Durumunuz:** Evli Bekar**6) Mesleğiniz :** .....

Aşağıda verilen ifadeler katılma derecenizi ilgili kutucuğa (X) işareti koyarak lütfen belirtiniz.

	HİÇBİR ZAMAN	NADİREN	BAZEN	SIKLIKLA	GENELLİKLE
<b>GÜVENLİK</b>					
1 - İnsan kaynakları çalışma alanında yetkili dışında bir çalışan, müşteri, tedarikçi vb. bulunur mu?					
2 - Çalışan özlük dosyalarının bulunduğu alana yetkili dışında bir çalışan, müşteri, tedarikçi vb. bulunur mu?					
3 - Çalışan özlük dosyalarının bulunduğu alana erişime sahip yetkili, şifre girme, kart okutma, zimmetli anahtar ile giriş sağlıyor mu?					
4 - Çalışanlar çalışma alanlarında fotoğraf çekmek ve ses kaydetmek için özel bir izin alıyor mu?					
5 - Güvenli alanlara giriş çıkış gerçekleşirken ziyaretçi defteri doldurulup, isim ve saatler kayıt altına alınmıyor mu?					
6 - Çalışanların şahsına ait taşınabilir cihazlar ile çalışma alanlarına girmesi bilgi yönetim sistemi yöneticisinden izin ile gerçekleşiyor mu?					
7 - Hassas bilgiler içeren depolama cihazları 'Hassas Ortam ve Teçhizat İmha Talimatı' na göre yetkili adına kayıt altına alınmıyor mu?					
8 - Ekranların, kullanmadığı zaman yetkisiz kişilerce görülmemesi için işletim sisteminin ekran kilitleme özelliği etkin hale getiriliyor mu?					
9 - Çalışanlar, hassas bilgi içeren dokümanlara yetkisiz kişilerin erişimini engellemek için temiz masa politikası uygulanıyor mu?					
10 - Çalışanlara, kendilerinden kaynaklı oluşan bilgi güvenliği zaafiyeti için disiplin prosedürü uygulanıyor mu?					
11 - Bilgilerin dağıtımı, naklinde özel güvenli paketlenme, güvenli kurye kullanma prosedürü uygulanıyor mu?					
12 - Bilgilerin elektronik ortamda işlenmesi, saklanması için sayısal imzalama veya şifreleme yöntemi kullanılıyor mu?					



13 - Kurum içi donanım ve uygulamalarında gerçekleşen bir güvenlik zaafiyeti işletim prosedürü dahilinde kayıt altına alınıyor mu?					
14 - Bilgi güvenliği zafiyeti gerçekleştiğinde düzeltici önleyici faaliyet formu oluşturuluyor mu?					
15 - Bilgi güvenliği zafiyeti gerçekleştiğinde yardım masasına kayıt yapılıyor mu?					
16 - Çalışanlar, taşınabilir ortamdaki bir bilgiyi kullanılmayacaksa bilgi yok etme prosedürü dahilinde imha ediyor mu?					
17 - Erişim Kontrol ve Ağ Hizmetleri Kullanım Talimatı oluşturularak bilgilere erişim sağlandığına dair takip yapılıyor mu?					
18 - Çalışanlar, hesaplarının güvenliğini şifre paylaşımında bulunmayarak, oturum kilitleyerek sağlıyor mu?					
19 - Çalışanlar sistemde yer alan bilgilere erişebilmeleri için taahhütname imzalıyor mu?					
20 - Çalışanların kullanıcı kimliklerini, iş gerekliliğine uygun bir şekilde kullandıklarının takibi yapılıyor mu?					
<b>SÜREÇ</b>					
21 - Çalışanlar ile işe giriş esnasında gizlilik sözleşmesi yapılıyor mu?					
22 - Çalışanlar ile işe giriş esnasında bilgi güvenliği politikası maddelerinin yer aldığı ve uyulmasının taahhüt edildiği bir sözleşme imzalanıyor mu?					
23 - İş sürekliliği planı oluşturularak olası iş akışı engelleyici durum yaşandığında oluşabilecek bilgi güvenliği zaafiyetini önlemek için belli periyotlarda toplantılar, değerlendirmeler yapılıyor mu?					
24 - Çalışanlar, Bilgi Güvenliği İhlal Olay Bildirimi ve Yönetim Talimatı'na göre bilgi işlem birimine raporlama yapıyor mu?					
25 - Dizüstü bilgisayar, masa üstü bilgisayar, belge, taşınabilir bellek gibi bilgi donanımı açısından önemli varlıkların korunması için talimatların yer aldığı bir belge çalışanlara imzalatılıyor mu?					
<b>BİLDİRİM</b>					
26 - Çalışanlar, kayıtlı taşınabilir cihazları firma dışına çıkarma durumunda güvenlik çalışanlarına durumu belirtici yazılı ve sözlü bir bildirimde bulunuyor mu?					
27 - Çalışanlara işe başlarken ve çalışma süresi içerisinde belli periyotlarda bilgi güvenliği farkındalık eğitimleri veriliyor mu?					

28 – Çalışanlara, ekranların, kullanmadığı zaman yetkisiz kişilerce görülmemesi için işletim sisteminin ekran kilitleme özelliği etkinleştirilmesi ile yazılı ve sözlü bilgilendirmede bulunuluyor mu?					
29 - Çalışanların kendilerine verilmiş olan kullanıcı ad ve şifrelerinin sadece kendileri tarafından kullanılması gerektiği bilgisi yazılı ve sözlü olarak veriliyor mu?					
30 - Temiz masa politikası ile ilgili çalışanlar yazılı ve sözlü olarak bilgilendiriliyor mu?					
31 - Çalışanlara, kullanmış oldukları masa çekmecelerini kilitli tutmaları gerektiği bilgisi yazılı ve sözlü olarak veriliyor mu?					
32 – Çalışanlar, ihtiyaç anında prosedürlere sürekli bir şekilde erişilebilen web, basılı ortamlardan ulaşabiliyor mu?					
33 – Çalışanlar ile olay yönetim prosedürleri belirlenerek güvenlik olayı başlangıcında, sırasında veya sonrasında yapılması gereken adımlar yazılı ve sözlü olarak paylaşılıyor mu?					
34 - İşlemler, prosedürler, veri yapıları gibi hassas bilgilerin bulunduğu sistem dokümantasyonuna ve bilgilerin elektronik kopyalarına iç ağ üzerinden erişim için çalışanlara yetkilendirme yazılı ve sözlü olarak yapılıyor mu?					
35 - E-postaların güvenliklerinin sağlanması amacıyla ‘Varlıkların Kullanımı Talimatı’ oluşturularak belirtilen maddelere göre hareket edilmesi için çalışanlar yazılı ve sözlü olarak bilgilendiriliyor mu?					
36 - Kurum bilgi sistemi içerisinde var olan herhangi bir bilginin kaybı olması durumunda çalışana, bilgi işlem ile anında irtibata geçmesi bilgisi yazılı ve sözlü olarak veriliyor mu?					
37 - Çalışanların sorumluluğu altında veya şahsına ait olan diz üstü - masa üstü bilgisayar, mobil cihazdan fotoğraftan yetkisi dışında doküman, belge paylaşımında bulunmaması ile ilgili bir taahhütname imzalıyor ve gerekli bilgilendirmeler yazılı/sözlü olarak yapılıyor mu?					
38 – Çalışana, kullanıcı bilgi güvenliği eğitimi veriliyor mu?					



## ÖZGEÇMİŞ

**Adı ve Soyadı:** Merve ÜNVER

**Doğum Yeri ve Tarihi:** 07/05/1992

### Öğrenim Durumu:

Derece	Alan	Üniversite	Yıl
Lisans	Çalışma Ekonomisi ve Endüstri İlişkileri	Gazi Üniversitesi	2006 - 2010
Yüksek Lisans	İşletme	Atılım Üniversitesi	2017 - 2019

### İş Deneyimi:

Çalıştığı Yer	Görev	Yıl
Geomatics Group	İnsan Kaynakları Uzmanı	2019
ABC Deterjan Sanayi ve Ticaret A.Ş.	İnsan Kaynakları Uzmanı	2018
Tesco Kipa Kitle Pazarlama Ticaret, Lojistik ve Gıda Sanayi A.Ş.	İnsan Kaynakları Uzmanı	2017

**Yabancı Diller:** İngilizce, Almanca

**E-Posta:** mmerveunver@gmail.com

**Telefon:** +90 553 469 32 49

**Tarih:**

# Merve Unver

## ORIJINALLIK RAPORU

% **10**

BENZERLIK ENDEKSİ

% **6**

İNTERNET  
KAYNAKLARI

% **0**

YAYINLAR

% **7**

ÖĞRENCİ ÖDEVLERİ

## BIRINCIL KAYNAKLAR

- 1** [bilgiguvenligidunyasi.blogspot.com](http://bilgiguvenligidunyasi.blogspot.com) İnternet Kaynağı % **1**
- 2** Submitted to Bahcesehir University Öğrenci Ödevi % **1**
- 3** [apache.beun.edu.tr](http://apache.beun.edu.tr) İnternet Kaynağı % **1**
- 4** Submitted to Marmara University Öğrenci Ödevi % **1**
- 5** Submitted to Hasan Kalyoncu Üniversitesi Öğrenci Ödevi % **1**
- 6** Submitted to Üsküdar Üniversitesi Öğrenci Ödevi <% **1**
- 7** Submitted to Istanbul Aydın University Öğrenci Ödevi <% **1**
- 8** Submitted to Beykent Üniversitesi Öğrenci Ödevi <% **1**
- 9** Submitted to TechKnowledge Turkey Öğrenci Ödevi <% **1**