
GAZİ ÜNİVERSİTESİ
Gazi
1926

ENERJİ SEKTÖRÜNDE BİLGİ GÜVENLİĞİ YÖNETİM SİSTEMLERİNİN ETKİ ANALİZİ VE SONUÇLARI

Beyzanur MADEN

YÜKSEK LİSANS TEZİ
ADLİ BİLİŞİM ANA BİLİM DALI

GAZİ ÜNİVERSİTESİ
BİLİŞİM ENSTİTÜSÜ

ARALIK 2024

ETİK BEYAN

Gazi Üniversitesi Bilişim Enstitüsü Tez Yazım Kurallarına uygun olarak hazırladığım bu tez çalışmasında;

- Tez içinde sunduğum verileri, bilgileri ve dokümanları akademik ve etik kurallar çerçevesinde elde ettiğimi,
- Tüm bilgi, belge, değerlendirme ve sonuçları bilimsel etik ve ahlak kurallarına uygun olarak sunduğumu,
- Tez çalışmasında yararlandığım eserlerin tümüne uygun atıfta bulunarak kaynak gösterdiğimi,
- Kullanılan verilerde herhangi bir değişiklik yapmadığımı,
- Bu tezde sunduğum çalışmanın özgün olduğunu,

bildirir, aksi bir durumda aleyhime doğabilecek tüm hak kayıplarını kabullendiğimi beyan ederim.

İmza

Beyzanur MADEN

...../……/……

ENERJİ SEKTÖRÜNDE BİLGİ GÜVENLİĞİ YÖNETİM SİSTEMLERİNİN ETKİ ANALİZİ VE SONUÇLARI

(Yüksek Lisans Tezi)

Beyzanur MADEN

GAZİ ÜNİVERSİTESİ

BİLİŞİM ENSTİTÜSÜ

Aralık 2024

ÖZET

Enerji sektörü, uluslararası alanda da kabul gördüğü üzere kritik altyapı sektörlerinden bir tanesidir. Bu sebeple sektör içerisinde bilgi güvenliğinin korunması oldukça fazla önem arz etmektedir. Ülkemizde enerji sektörüne mensup kurum ve kuruluşlarda, bilgi güvenliğini korumaya yönelik bilgi güvenliği yönetim sistemlerinin mevcut olduğu bilinmektedir. Bu çalışma sektördeki ilgili kurum ve kuruluşların bilgi güvenliği yönetim sistemlerinin ne derece etkin olduğunun kavranabilmesi amacıyla hazırlanmıştır. Bilgi güvenliği yönetim sistemi çalışanları, yöneticiler ve bu kapsamların dışında kalan personel grupları için ayrı ayrı hazırlanan likert tipi anketler, Enerji ve Tabii Kaynaklar Bakanlığı (ETKB) teşkilatı ve bağlı/ilgili kuruluşlarındaki çalışanlara kurumsal e-posta üzerinden çevrimiçi olarak gönderilerek katılım sağlamaları için sunulmuştur. Toplamda 181 personelden elde edilen geri dönüşlerin ardından, her anket grubu kendi içerisinde analiz edilmiştir. Personel anketinin sonuçları ETKB Bilgi İşlem Dairesi birimleri bazında incelenirken; bilgi güvenliği çalışanlarına ve yöneticilere yönelik anketlerin sonuçları doğalgaz, elektrik, kömür, maden, nükleer, petrol ve son olarak merkez teşkilat bazında incelenmiştir. Sektördeki çalışanların bakış açısını irdeleyen anketler sonucunda, olumlu bir tablonun ortaya çıktığı görülmüştür. Bilgi güvenliği sistemlerinin yapısı gereği her zaman iyileştirmeye açık olması sebebiyle, tespit edilen hususlardaki önerilere çalışmanın Sonuç kısmında yer verilmiş, özellikle bilgi güvenliği hususundaki bilincin geliştirilmesine yönelik yapılabilecek çalışmaların başında gelen farkındalık eğitimlerinin düzenlenmesinin yararlarına değinilmiştir. Bu çalışmanın; literatürde enerji sektöründeki bilgi güvenliğinin mevcut durumunun tespitine yönelik çalışma açığını kapatması ve diğer kritik altyapı sektörleri için de örnek teşkil etmesi temenni edilmektedir.

Bilim Kodu	:	92401
Anahtar Kelimeler	:	Enerji sektörü, bilgi güvenliği, bilgi güvenliği yönetim sistemi, ISO/IEC 27001
Sayfa Adedi	:	117
Danışman	:	Prof. Dr. Mustafa ALKAN

IMPACT ANALYSIS AND RESULTS OF INFORMATION SECURITY MANAGEMENT SYSTEMS IN THE ENERGY SECTOR

(M. Sc. Thesis)

Beyzanur MADEN

GAZİ UNIVERSITY

INSTITUTE OF INFORMATICS

December 2024

ABSTRACT

The energy sector is one of the critical infrastructure sectors, as accepted internationally. For this reason, protection information security is of great importance within the sector. It is known that information security management systems are available in institutions and organizations affiliated with the energy sector in our country to protect information security. This study was prepared to understand how effective the information security management systems of the relevant institutions and organizations in the sector are. Likert-type surveys prepared separately for information security management system employees, managers, and personnel groups outside these scopes were sent online to employees in the Ministry of Energy and Natural Resources (MENR) organization and its affiliated/related organizations via corporate e-mail and presented for their participation. After the feedback obtained from a total of 181 personnel, each survey group was analyzed within itself. While the results of the personnel survey were examined based on MENR Information Processing Department units; the results of the surveys for information security employees and managers were examined based on natural gas, electricity, coal, mining, nuclear, oil, and finally the central organization. As a result of the surveys examining the perspectives of employees in the sector, a positive picture was observed. Since information security systems are always open to improvement due to their nature, suggestions on the identified issues are included in the Conclusion section of the study, and the benefits of organizing awareness training, which is one of the primary studies that can be conducted to develop awareness on information security, are mentioned. It is hoped that this study will fill the gap in the literature regarding the determination of the status of information security in the energy sector and will also serve as an example for other critical infrastructure sectors.

Science Code	:	92401
Key Words	:	Energy sector, information security, information security management system, ISO/IEC 27001
Page Number	:	117
Supervisor	:	Prof. Dr. Mustafa ALKAN

TEŞEKKÜR

Yüksek lisans eğitimim boyunca engin tecrübesinden faydalandığım ve bu çalışmanın meydana çıkmasında yol gösterici olması ile her zaman minnettar kalacağım sayın danışmanım Prof. Dr. Mustafa ALKAN hocama; çalışmanın özellikle anketler kısmı başta olmak üzere bütün aşamalarıyla yakından alakadar olan ve desteğini hiçbir zaman esirgemeyen Enerji ve Tabii Kaynaklar Bakanlığı Bilgi İşlem Dairesi Başkanı Sayın Hakkı TOK'a; kurum ve kuruluşlardan anketlere katkıda bulunmuş olan tüm mesai arkadaşlarıma çok teşekkür ederim.

Ayrıca hem akademik hem de profesyonel hayatında gösterdiği azim ve kararlılıkla benim için bir idol olan Türk enerji sektörünün duayenlerinden meslektaşım, babam, Muhammet MADEN'e; eğitime ömrünü adamış, evlatlarına ve evlatlarından ayırmadan yetiştirdiği sayısız öğrencinin her birine, vatanı ve milletine hizmetin iyi eğitimli bireyler olmaktan geçtiği fikrini aşılamış, hayatımdaki ateşleyici güç olan annem Gülay MADEN'e; aramızdaki sekiz yıllık yaş farkını ne zaman erittiğini kestiremediğim, ülkülerimiz hakkında ettiğimiz son derece derin ve ciddi sohbetlerin yanı sıra hayatımdaki en eğlenceli figür olan küçük kardeşim Yuşa MADEN'e teşekkürlerin en büyüğünü borç bilirim.

İÇİNDEKİLER

Sayfa

Sayfa

ÇİZELGELERİN LİSTESİ

Çizelge **Sayfa**

ŞEKİLLERİN LİSTESİ

Şekil **Sayfa**

SİMGELER VE KISALTMALAR

Bu çalışmada kullanılmış simgeler ve kısaltmalar, açıklamaları ile birlikte aşağıda sunulmuştur.

Simgeler	**Açıklamalar**
f	Frekans (sıklık) değeri
%	Yüzdelik değer
α	Cronbach Alpha katsayısı
σ	Varyans

Kısaltmalar	**Açıklamalar**
AB	Avrupa Birliği
ABD	Amerika Birleşik Devletleri
AFAD	Afet ve Acil Durum Yönetimi Başkanlığı
A.Ş.	Anonim Şirketi
BGYS	Bilgi Güvenliği Yönetim Sistemi
BİGR	Bilgi ve İletişim Güvenliği Rehberi
BOTAŞ	Boru Hatları ile Petrol Taşıma A.Ş.
BT	Bilgi Teknolojileri
DDO	Dijital Dönüşüm Ofisi
DDOS	Distributed Denial of Service
DOS	Denial of Service
DCS	Distrubuted Control System
DKS	Dağıtılmış Kontrol Sistemleri
EKS	Endüstriyel Kontrol Sistemleri
EPDK	Enerji Piyasası Düzenleme Kurumu
ETKB	Enerji ve Tabii Kaynaklar Bakanlığı
ETİ MADEN	Eti Maden İşletmeleri Genel Müdürlüğü
EÜAŞ	Elektrik Üretim A.Ş. Genel Müdürlüğü
IEC	International Electrotechnical Commission

ISO	International Organization for Standardization
IT	Bilgi teknolojileri
ITU	International Telecommunication Union
LPG	Likit petrol gazı
MAPEG	Maden ve Petrol İşleri Genel Müdürlüğü
MITM	Man In The Middle
MTA	Maden Tetkik ve Arama Genel Müdürlüğü
MTU	Merkezi Terminal Ünitesi
NIST	National Institute of Standards and Technology
NDK	Nükleer Düzenleme Kurumu
OT	Operasyonel Teknolojiler
PLC	Programmable Logic Controller
RTU	Remote Terminal Unit
SCADA	Supervisory Control and Data Acquisition
SQL	Structured Query Language
TDK	Türk Dil Kurumu
TEDAŞ	Türkiye Elektrik Dağıtım A.Ş. Genel Müdürlüğü
TEİAŞ	Türkiye Elektrik İletim A.Ş. Genel Müdürlüğü
TEMSAN	Türkiye Elektromekanik Sanayi A.Ş.
TENMAK	Türkiye Enerji Nükleer ve Maden Araştırma Kurumu
TKİ	Türkiye Kömür İşletmeleri Kurumu Genel Müdürlüğü
TPAO	Türkiye Petrolleri Anonim Ortaklığı Genel Müdürlüğü
TSE	Türk Standartları Enstitüsü
TTK	Türkiye Taşkömürü Kurumu Genel Müdürlüğü
YGG	Yönetimin Gözden Geçirmesi

1. GİRİŞ

Bir ülkenin gelişimi, vatandaşlarının bilgi toplumu olabilmek adına oluşturduğu bilincin ne kadar kuvvetli olduğuna bağlı iken, bilgi toplumu olabilmek hem fiziksel hem de kültürel değişimin gerçekleşmesine bağlıdır [1]. Bu kapsamda süreklilik oldukça önemli bir olgudur ve bilginin korunma ihtiyacının giderilmesiyle sağlanmaktadır. Bilgi güvenliğinin sürekliliğine dayanan süreçlerin tek bir çatı altından yürütülmesi ise bir yönetim sistemine sahip olma mecburiyeti oluşturmaktadır. Bilgi güvenliği yönetim sistemleri işte bu doğrultuda hayatımızda varlığını sürdürmektedir.

Bununla birlikte zafiyetlerden kaynaklanan güvenlik ihlallerinin çoğunlukla bireylerin eksikliklerinden meydana geldiği düşünüldüğünde bilgi güvenliğini korumak adına yalnızca teknik çözümlerin ve güçlendirilmiş siber güvenlik altyapıların yeterli olmayacağı açıktır. Bilgi güvenliği yönetim sistemleri bu yönüyle de devreye girmekte ve her açıdan bilginin korunmasına dair sürdürülen faaliyetleri kapsamaktadır.

Bir ülkenin hayati önem taşıyan sektörlerinde, kritik altyapılarında bilgi güvenliği süreçlerinin aksaklığa pay vermeden yürütülebilmesi için bu sistemlere ihtiyaç olduğu yadsınamaz bir gerçektir. Çünkü bilgi güvenliği ihlali geri dönüşü olmayan felaketlere yol açabilmektedir. Dünya üzerinde de bu duruma örnek verilebilecek birçok olay meydana gelmiştir. Ülkelerin kendileri için tanımladığı her bir kritik altyapı için gerçekleştirilmiş olan birbirinden farklı saldırıların kamunun düzenini bozduğu bilinmektedir. Örneğin; ülkelerin ulaşım sistemlerine yönelik saldırılarda vatandaşın çeşitli ihtiyaçlarına ulaşma yolları tabiri caizse felç edilebilmiş, su sistemlerine yönelik saldırılarda yine temel ihtiyaçlarının karşılanamamasından ötürü toplum sağlığı riske atılabilmiştir.

Kritik altyapılardan biri olan enerji sektöründe de uluslararası alanda büyük yankı uyandırmış birçok olay yaşanmıştır. Birçoğunda doğrudan endüstriyel kontrol sistemlerinin hedef alındığı saldırılardan başarılı olanları ülkelerin refahını zarara uğratmakla kalmamış halkın sağlığını ve güvenliği tehlikeye atılarak, çeşitli temel ihtiyaçlarının kesintiye uğramasına neden olmuştur. Bu sebepten enerji sektöründe de güvenliğin hayati önem taşıdığı bilincine ulaşılmıştır ve bilgi güvenliğinin korunmasına dair çeşitli faaliyetlerin gerçekleştirilmektedir.

Tüm sektörlerde bilgi güvenliği yönetim sistemlerinin kurulması ve yönetilmesi açısından hazırlanan yol gösterici dokümanların yardımıyla yürütülen sistemlerin en ufak hatayı dahi

göz ardı etmeden güvenlik unsurlarının kapsama alınması hedeflenmektedir. Buradan yola çıkarak bilgi güvenliği yönetim sistemleri için bir kurum ya da kuruluş temel ihtiyacı olduğu söylenebilir. Bu ihtiyacın kurum ya da kuruluşun bünyesinde yer alan her bir öge için benimsenmesinin ise sistemin en önemli mecburiyeti olduğu düşünülmektedir. Çünkü sistemin sağlıklı şekilde yürütülebilmesi kurum bünyesinde yer alan herkesin eşgüdümlü olarak süreçlere dahil olmasına bağlıdır.

Enerji sektörü için bakıldığında literatürde veya pratikte bilgi güvenliği yönetim sistemlerinin sektörde görev alan kimselerin perspektifinden ne durumda olduğuna dair hazırlanmış bir çalışmaya rastlanmamıştır. Oysa sistemin sağlıklı şekilde yürütülebilmesi, bunun yanı sıra düzeltme ve iyileştirmelerin doğru şekilde yapılabilmesi için mutlaka sisteme dair geri dönüşleri barındıran fikirlerin dikkate alınması gerekmektedir.

Bilgi güvenliği yönetim sistemlerinde birbirinden farklı bakış açısına sahip olabilecek grupların bulunduğu düşünülmektedir. Çünkü daha önce de söz edildiği gibi kurumsal bilgi güvenliğinden yalnızca, kurumun bilgi güvenliği yönetimi hususunda görev alan personelini sorumlu tutmak yanlış bir yaklaşım olacaktır. Bilgi güvenliği yönetim sistemleri için hazırlanan uluslararası dokümanlarda kurum yöneticileri ile birlikte bütün personele yönelik direktiflere yer verilmektedir. Bu düşünce yapısı ile temele indirgendiğinde ortaya şu üç grup çıkmıştır:

a) Görev aldıkları kurumda bilgi güvenliği yönetim sistemi ile ilgili faaliyetleri yürüten çalışanlar
b) Kurumda yönetici pozisyonunda görev alan kişiler
c) Görev aldıkları kurumda doğrudan bilgi güvenliği yönetim sistemleri çalışmalarında etkin rol oynamayan personel

Bu çalışmanın hazırlanmasındaki temel amaç bu üç grubun enerji sektöründe bilgi güvenliği yönetim sistemlerine dair bakış açısının değerlendirilebilmesi, mevcut durumun ölçülebilmesi ve bunun sonucunda ihtiyaç duyulması halinde önerilerde bulunulabilmesidir.

Bakış açısının değerlendirilebilmesi için en etkili yöntemin anket çalışması olacağı düşünülmüştür. Bahsi geçen üç grup için, bilgi güvenliği yönetim sistemleri ile ilgili kendilerini ilgilendiren hususlarda likert tipi ölçek kullanılmak suretiyle sorular hazırlanmıştır. Sektörde yer alan kurumların ilgili gruplarına dağıtılan anketlerin sonuçlarının değerlendirilmesi ve bu kapsamda çalışmanın bilgi güvenliği yönetim

sistemlerinin mevcut durumunun ortaya koyulması konusundaki amacının gerçekleştirilmesi hedeflenmiştir.

Çalışmada öncelikle, çalışmanın üzerine inşası için temel oluşturan bazı kavramların açıklanması için bir bölüme yer verilmiştir. Bölüm içerisinde öncelikle bilgi ve bilgi güvenliği gibi kavramların tanımlarına yer verilmiştir. Bilgi kavramı açıklanırken; bilgi türleri, veri ve özbilgi de tanımlanmıştır. Bilgi güvenliği hususunda ise öncelikle üç temel unsuruyla yani gizlilik, bütünlük ve erişilebilirlik ile alakalı açıklamalara, ardından da bilgi güvenliğinin diğer temel ilkelerinden bahsedilmiştir. Bu tanımlamaların ardından kriptolojiden ve tarihsel gelişiminden söz edilmiştir. Daha sonra kritik altyapılar ile ilgili bazı açıklamalara yer verilmiştir. Amerika Birleşik Devletleri, Avrupa Birliği, Japonya ve Türkiye'nin kritik altyapı kapsamına aldığı sektörler sıralanmıştır. Kritik altyapıların açıklanmasının ardından endüstriyel kontrol sistemleri alt başlığı atılmış ve gerekli tanımlamalar yapılmıştır. Endüstriyel kontrol sistemlerinin bünyesinde bulunan SCADA, DCS, PLC gibi çeşitli terminaller ve sistemlere de bu bölümde yer verilmiştir. Kavramsal Çerçeve bölümünün dördüncü ve sonuncu alt başlığında ise bilgi güvenliği yönetim sistemleri açıklanmıştır. Bu kısımda PUKÖ döngüsünden de söz edilmiştir. Bu döngü kapsamında planlama, uygulama, kontrol etme ve önlem alma aşamalarının sürekli bir döngü içerisinde yürütülmesine dair açıklamalar detaylıca anlatılmıştır.

Kavramsal Çerçeve bölümünü takiben enerji sektöründe bilgi güvenliği yönetim sistemlerinin neden önemli olduğunu açıklamaya yönelik bir bölüm oluşturulmuştur. Bu bölüm içerisinde enerji sektörü, siber saldırı yöntemleri ve enerji sektöründe gerçekleşen saldırılardan bazılarını açıklayan alt başlıkları barındırmaktadır. Enerji sektörü alt başlığında Enerji ve Tabii Kaynaklar Bakanlığı bağlı ve ilgili kuruluşları hakkında misyonlarını da açıklayan kısa bilgiler bulunmaktadır. Siber saldırı yöntemlerinden en çok tercih edilenler açıklandıktan sonra uluslararası alanda, enerji sektörü bünyesinde meydana gelen, kamuoyunda yankı uyandırmış saldırılardan bazılarına yer verilmiştir.

Daha sonra bilgi güvenliği yönetim sistemlerinin kurulması ve yürütülmesi için yol gösterici olan çeşitli dokümanların tanıtıldığı bir bölüm hazırlanmıştır. Bölümün kapsamında ulusal ve uluslararası çerçevede bilgi güvenliği standartları ve rehberlerine ilişkin açıklamalar bulunmaktadır.

Bu bölümlerden sonra ise literatür özetine yer verilen bir bölüm hazırlanmıştır. Literatür taramasının nasıl yapıldığından, nelere dikkat edildiğinden, hangi anahtar kelimelerin kullanıldığından bahsedilmiştir. Bu çalışmanın hazırlanması esnasında faydalanılan kaynaklardan söz edilmiştir.

Literatür özeti hakkındaki bölümünden sonra bu çalışmanın yöntemi ve bulgularının açıklandığı bölümlere yer verilmiştir. Daha önce bahsedildiği gibi farklı gruplara yönelik, kendi içerisinde değişiklik gösteren üç ayrı anket hazırlanmıştır. Bu anketlerin soruları ve hedef kitleleri yöntemin yazıldığı bölümde açıklanmıştır. Katılımcıların anketlere sağladıkları geri dönüşün ardından ilgili analizler gerçekleştirilmiştir. Gruplar dikkate alınarak gerçekleştirilen analizler bulguların açıklandığı bölümde gösterilmiştir.

Sonuç bölümünde ise bulgulara yönelik çıkarımlar özetlenmiştir. Farklı grupların bakış açısından enerji sektöründeki bilgi güvenliği yönetim sistemlerine yönelik mevcut durum ortaya koyulmuştur. Bu kapsamda önerilere yer verilerek çalışma sonlandırılmıştır.

2. KAVRAMSAL ÇERÇEVE

Bu bölümde; bilgi, veri, bilgi güvenliği, kritik altyapılar, endüstriyel kontrol sistemleri ve bilgi güvenliği yönetim sistemleri hususlarında tanımlamalara ve açıklamalara yer verilmiştir. Bu kavramların açıkça ifade edilmesi çalışmanın geri kalanı için önemli görülmektedir.

2.1. Bilgi ve Bilgi Güvenliği Kavramlarının Tanımı

Türk Dil Kurumu'na göre bilgi; "İnsan aklının erebileceği olgu, gerçek ve ilkelerin bütünü" olarak tanımlanmıştır [2]. İngilizce *information* terimine karşılık gelen bilgi kavramı; bir hususa dair meydana gelen belirsizliği indirgeyen kavram olarak da tanımlanabilir [3]. Felsefeden bilişime birçok alanda, bilginin farklı tanımları mevcuttur. Bu tanımlar kişinin perspektifine ve ilgi alanına göre değişkenlik gösterebilmektedir. Bilginin çeşitlerinin olduğu kabul edilmektedir. Bahsi geçen çeşitler; gündelik, teknik, bilimsel, felsefi, sanatsal ve dinsel şeklinde sıralanabilmektedir.

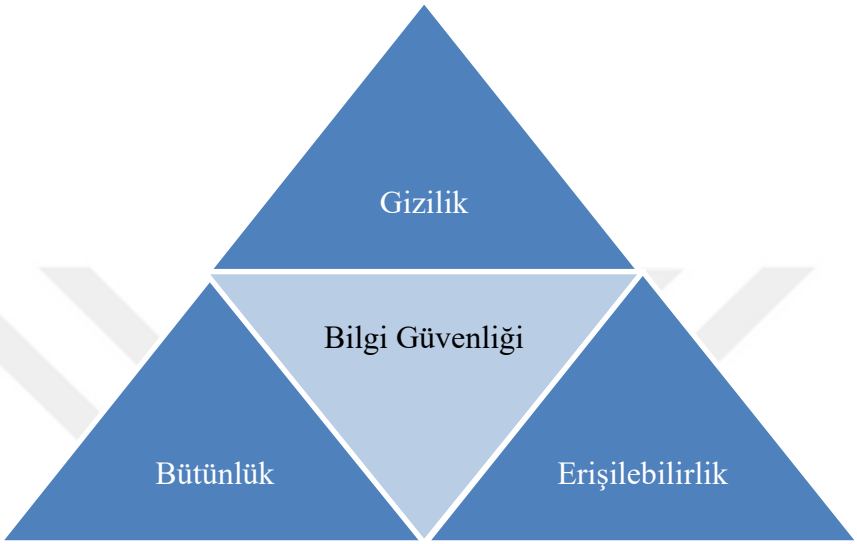
Bu çeşitlere ek olarak tecrübeye dayanan özbilgi kavramı da göz önünde bulundurulmalıdır. Özbilgi; İngilizce *knowledge* kelimesinin karşılığıdır. Çeşitli yöntemlerle edinilen bilginin fark edilmesi ve anlamlandırılması manasına gelmektedir [3].

Türkçeye *knowledge* ve *information* terimlerinin aynı kelimeyi yani bilgi kavramını betimleyecek şekilde çevrilmesi sebebiyle kavram karmaşası yaşanabilmektedir. Dolayısıyla özbilgi kelimesinin literatürde ve bilişim sektöründe daha fazla yer edinmesinin gerekli olduğu düşünülmektedir.

Bu çalışmada bilgi kavramının bilişim sektöründeki ifadesi baz alınacaktır. Dolayısıyla bilgi için "verinin bir üst formu, işlenmiş ve anlamlandırılmış hali" tanımlaması yapılabilir. Bu noktada elbette ki veri kavramının da tanımlanması gereklidir. Veri "bütünlüğü ve yapısı bozulmamış, bir noktadan diğerine iletilmesi istenen metin, ses, görsel ve video" şeklinde ifade edilebilmektedir.

Bilgi güvenliği; bilgilere izinsiz şekilde erişime, bilgilerin değiştirilmesine tahrip edilmesine veya yok edilmesine önlem olması amacıyla geliştirilen araçlar ve uygulanan süreçleri kapsamaktadır. Birçok farklı kaynakta, birbirinden değişik şekilde tanımlanmasına karşın, bu tanımları ortak paydada buluşturan unsurları mevcuttur. Bu unsurlar; gizlilik, bütünlük ve erişilebilirlik olarak sıralanmaktadır.

Gizlilik, bütünlük ve erişilebilirlik üçlüsü genellikle üçgen şeklinde bir şema olarak görselleştirilmektedir. Kısaca; İngilizcede gizlilik anlamına gelen *confidentiality*, bütünlük anlamına gelen *integrity* ve erişilebilirlik anlamına gelen *availability* kelimelerinin baş harflerinden oluşan "CIA" kelimesiyle tanımlanan bu üçlüden oluşan şemaya CIA şeması adı verilmektedir [4]. Aşağıda, Şekil 2.1'de, CIA şeması gösterilmiştir.



Şekil 2.1 CIA şeması

Gizlilik, yetkisi olmayan kişilerin bilgiyi elde etmesinin engellenmesi; bütünlük, bilginin göndericiden çıktığı haliyle alıcıya ulaşması; erişilebilirlik ise bilginin yetkisi olan kişiler tarafından sürekli olarak tam ve eksiksiz şekilde ulaşılabilir ve kullanılabilir olması olarak tanımlanmaktadır [5].

Kurum ve kuruluşlar bu unsurlardan hangisinin kendileri için öncelikli olduğuna karar vermelidir. Ancak bu geriye kalan unsurların önemsiz olduğu anlamına gelmemektedir. Çünkü bahsi geçen güvenlik prensiplerinin tamamının sağlanması durumunda bilgi güvenliğinin varlığı söz konusu olabilmektedir.

Bilgi güvenliğinin üç temel unsuruna ek olarak başka unsurların da söz konusu olduğu bilinmektedir. İlerleyen bölümlerde daha detaylı şekilde açıklanacak olan, uluslararası alanda en yaygın bilgi güvenliği standartlarını bünyesinde barındıran ISO/IEC 27000 ailesinde hem bu üç unsur tanımlanmış hem de diğer ilkelere yer verilmiştir. Bahsi geçen belgede yer verilen diğer temel ilkeler; güvenilirlik (*reliability*), inkâr edememe (*non-repudiation*), kayıt tutma (*log accountability*) ve kimlik tespiti (*authentication*), olmak üzere sıralanabilmektedir.

Bilgi güvenliğinin korunmasından söz edilince akla şifreleme faaliyetleri gelmektedir. Şifreleme manasına gelen kriptografi (*cryptography)* kelimesinin kökenine bakıldığında; Antik Yunan dilinde gizli anlamına gelen *kripto* kelimesiyle yazmak anlamına gelen *grafi* kelimelerinin birleştirilmesiyle anlamlı hale getirildiği görülmektedir.

Kriptografiden söz edildiği yerde kriptoanaliz kavramı da devreye girmektedir. Çünkü kriptoanaliz şifrelenmiş mesajların çözülmesi anlamını taşır. Yani kriptografi ve kriptoanaliz birbirinin tam tersidir. Bir diğer ifadeyle kriptografi için "şifreleme sanatı", kriptoanaliz için ise "şifreyi çözme sanatı" denilebilmektedir [6]. Kriptografi ve kriptoanaliz birlikte kriptolojiyi oluşturmaktadırlar.

Kriptoloji yani şifreleme bilimi; gönderilen mesajın, gönderici ile alıcı arasındaki gizliliği koruyarak gönderilmesini amaçlayan ve mesajın güvenliğini sağlamayı hedefleyen bir bilim dalıdır. Kelimenin kökeni yine Antik Yunan diline dayanmaktadır. Daha önce bahsedildiği gibi gizli anlamına gelmekte olan *kripto* kelimesi bu sefer *logos* kelimesiyle birleştirilmiştir [7]. Logos felsefede de kendine yer bulmuş bir tabirdir ve etimolojik olarak "söz söylemek, okumak" anlamlarına gelse de "usla kavrama" manası taşımaktadır [8].

Şifrelemenin tarihi ise çok eski zamanlara dayanmaktadır. Çünkü insanoğlu var olduğu süre boyunca, tarihin bütün sahnelerinde mahremiyetine önem vermiştir. İnsanın yapısından gelen bu davranış eğilimi zamanla stratejik eylemlere dökülmüş ve kriptoloji çalışmalarını meydana getirmiştir. Yaklaşık 4000 yıldır bu alandaki çalışmaların var olduğu bilinmektedir.

Dünya üzerinde birçok millet çeşitli kriptografi ve kriptoanaliz çalışmaları yürütmüşlerdir. Ancak Çin medeniyetinde dikkate değer bir çalışmaya rastlanmamıştır. Bunun sebebinin Çin alfabesinin fazlasıyla zor ve karmaşık olmasından kaynaklandığı düşünülmektedir.

David Kahn "*The Codebreakers*" isimli eserinde kriptoloji faaliyetlerinin tarihçesine yer vermiştir. Bu çalışmada da kriptolojinin tarihçesinden bahsederken bu eser kaynak olarak alınmaktadır. Kahn'a göre Kriptoloji alanında 4000 yıldır meydana gelen önemli gelişmeler şu şekildedir [9]:

- MÖ 1900'ler: Tespit edilen ilk kriptoloji eylemine Mısır'da rastlanmıştır. Mısırlı bir kâtibin, daha önce kullanılmadığı tespit edilen hiyerogliflerle oluşturduğu metin ilk yazılı kriptografik doküman olarak kabul edilmiştir.
- MÖ 1500: Bir Mezopotamya tabletinin, çömlekçilikle ilgili sırlar barındıran şifreli bir formül içerdiği bilinmektedir.

- MÖ 600 – 500 yılları arası: Eski Ahit'de yer alan Jeremiah kitabını yazan İbrani katipler 'Atbash' olarak bilinen bir şifreleme yöntemi kullanmışlardır. Bu şifreleme metodu alfabeyi tersinden yazarak yerine koyma şeklinde gerçekleştirilmektedir. Atbash'in o zamanlarda kullanılan İbranice şifrelemelerinden biri olduğu bilinmektedir.
- MÖ 487: Askeri alandaki ilk kriptografik faaliyetler bu zamanlarda gerçekleşmiştir. Spartalılar geliştirdikleri bir teknik sayesinde askeri alanda avantaj sağlamayı amaçlamışlardır. Belli kalınlıkta bir çubuğa sarılmış olan ince bir deri şeride mesajlarını yazdıktan sonra, şerit çubuktan çıkartılmaktadır. Şifrenin çözülmesindeki tek yol şeridin tekrar aynı kalınlıkta bir çubuğa sarılmasıdır.
- MÖ 50-60: Askeri alanda bir diğer önemli kriptografik gelişme bu tarihlerde Roma'da meydana gelmiştir. Büyük Roma İmparatoru olan Julius Caesar; komutanları ile haberleşmek için Atbash şifreleme metoduna benzer ancak onun kadar kuvvetli olmayan bir metot kullanmıştır. Caesar şifreleme metodu; alfabedeki harflerin 3 harf sonrasındaki harfin yerine kullanılmasıyla şifrelemeye dayanan bir yöntemdir. Basit bir metot olmasına rağmen, döneminin ihtiyaçlarını karşıladığı bilinmektedir.
- 718: Abu `Abd al-Rahman al-Khalil ibn Ahmad ibn `Amr ibn Tammam al Farahidi al-Zadi al Yahmadi isimli Arap dilinin mevcut en eski sözlüğünün de yazarı olduğu bilinen filolog, dönemin Bizans İmparatoru için çözdüğü Yunan dilinde hazırlanmış şifreli bir metinden esinlenerek kriptografi üzerine bir kitap yazmıştır. Kitabın şu an kayıp olduğu bilinse de uyguladığı düşünülen metodun Enigma şifrelemelerinde dahi kullanıldığı söylenmektedir.
- 1000-1200: Gazneliler'in üst düzey yönetimde görev alacak kimselere, kişisel bir şifre verdiği bilinmektedir.
- 1363: Batıda Ortaçağda başlayan kriptoloji faaliyetleri, kendini ilk önce 1363 yılında Kardinaller ile Papa arasında kullanılarak göstermiştir.
- 1412: Abdullah Kalkaşendi 1412 tarihinde tamamladığı, Subhu'l Aşa isimli 14 ciltten oluşan Arapça ansiklopedinin kriptoloji ile ilgili bölümlerinde harf frekanslarını ve bir arada bulunmayan harf kümelerinin listesi bulunmaktadır.
- 1466-1467: Leon Battista Alberti; iç içe geçen iki diskten oluşan bir şifreleme cihazı ile, 1800'lü yıllara kadar kırılamadığı bilinen ilk çok alfabeli şifreyi icat etmiştir.

- 1586: Blaise de Vigenere; otomatik anahtar sistemi yani bir önceki şifreli ya da düz metnin kelimelerinin geçerli metnin anahtarında kullanılması ile ilgili bir kitap yazmıştır. Günümüzde bu yöntemin hala kullanıldığı alanlar olduğu bilinmektedir.
- 1623: Sir Francis Bacon; günümüzde kendi adını taşıyan ve karakter tipi değişikliğine dayanan bir şifreleme metodu geliştirmiştir.
- 1790: Thomas Jefferson, daha sonraki yıllarda çeşitli yerlerde tekrar kullanılmak üzere geliştirilen tekerlek şifresini icat etmiştir.
- 1854: Charles Wheatstone; arkadaşı Playfair'in adını taşıyan, kullanımı kolay bir digrafik şifre oluşturmak için anahtarlı bir harf dizisi kullanan şifreyi icat etmiştir.
- 1861: Fredrich W. Kasiski, çok alfabeli şifrelerde yer alan tekrar eden grupları kullanarak şifre kırma yöntemini anlatan bir kitap yayınlamıştır.
- 1914: 1.Dünya Savaşı'nın başlamasıyla, özellikle İngilizler ve Fransızlar tarafından kullanılan çeşitli yöntemlerle kriptografinin yine askeri amaçlarla kullanımının örnekleri görülmüştür.
- 1917: Gilbert S. Vernam ve Joseph Mauborgne; "One-Time-Pad" adı verilen rastgele ve tekrarlanmayan bir anahtarı kullanabilen alfabetik şifreleme sistemi geliştirmişlerdir.
- 1923: 2.Dünya Savaşı sırasında Alman hükümeti tarafından geliştirilecek olan Enigma makinesi, ticari amaçlar güdülerek Arthur Scherbius tarafından icat edilmiştir. Savaş esnasında Enigma makinesi ile şifrelenen metinlerin kırılması için İngiltere'de karşı istihbarat çalışmaları yürütülmüş ve Alan Turing ile ekibi tarafından her türlü şifrenin kırılması sağlanmıştır.
- 1970: Dr. Horst Feistel, IBM Watson Araştırma Laboratuvarında Lucifer şifresini geliştiren bir araştırma projesi yürütmüştür.
- 1976: Lucifer şifresinin temelini oluşturduğu "Data Encyrption Standard" (DES), Amerika Birleşik Devletleri (ABD) tarafından FIPS 46 (Federal Information Processing Standard) olarak ilan edilmiştir.
- 1976: Whitfield Diffie ve Martin Hellman; "New Directions In Cryptography" isimli çalışmalarını yayımlayarak, açık anahtar sistemini tanıtmışlardır.
- 1978: Ronald L. Rivest, Adi Shamir ve Leonard M. Adleman; büyük sayıları çarpanlarına ayırmanın zorluğuna dayanan pratik bir açık anahtar şifresi olan RSA algoritmasını geliştirmişlerdir.

- 1990: Xuejia Lai ve James Massey; DES'in yerine geçmek üzere önerilecek IDEA algoritmasını bulmuşlardır.
- 1991: Phil Zimmerman tarafından FBI'ın vatandaşların iletişimlerinin açık metnine erişim talep etme tehdidine karşılık olarak, vatandaşa yüksek güvenlik sunan PGP'nin ilk versiyonu yayınlanmıştır.
- 1995: ABD'nin standardizasyon kurumu olan *National Institute of Standards and Technology* (NIST) tarafından; SHA-1 (Secure Hash Algorithm) algoritması standart şeklinde yayımlanmıştır.
- 1997: NIST; DES algoritmasının yerine geçebilecek bir simetrik algoritma geliştirilmesi için yarışma başlatmıştır. Joan Daemen ve Vincent Rijmen'in Rijndael algoritması ile yarışmayı kazanmalarının ardından geliştirdikleri algoritma 2001 yılında AES (Advanced Encryption Standard) adını alarak standard şeklinde yayınlanmıştır.

Buradan görülebileceği üzere dünyanın dört bir yanından çeşitli toplumlar, kendilerine uygun sebeplerle kriptoloji üzerine faaliyetler göstermiş ve tabiri caizse koydukları her bir tuğla ile bu bilimin günümüzde bu denli önemli hale gelmesinin inşasında rol oynamışlardır. Bununla beraber birçok alanda gelişme gösterdiği bilinen Çin medeniyeti, alfabelerinin karmaşıklığı ve zorluğu sebebiyle kriptoloji alanında kayıtlara geçebilecek bir katkıda bulunamamıştır. Bugüne geldiğimizde ise, teknolojinin her geçen gün gelişmesi ile kriptolojik faaliyetler de hızla gelişmeye devam ettiği söylenebilmektedir.

2.2. Kritik Altyapılar

1996 yılında, o zamanki Amerika Birleşik Devletleri (ABD) Başkanı Bill Clinton tarafından kurulan "*The President's Commission on Critical Infrastructure Protection"* (PCCIP) tarafınca kaydedilen kritik altyapı kavramı, günümüzde de önemi katlanarak göz önünde bulundurulan bir kavram olarak kendine yer edinmiştir [10]. ABD'de atılan bu adımın ardından yıllar içinde başta Avrupa Birliği (AB) olmak üzere dünyanın geri kalanında da kritik altyapılarla ilgili aksiyonlar alınmaya başlandığı bilinmektedir.

Ülkelere göre kritik altyapı kapsamı değişiklik göstermektedir. ABD; kritik altyapı kapsamına Yurt Güvenlik Teşkilatı tarafından yayımlanan Ulusal Altyapı Koruma Planı'nda belirlenmiş 18 altyapıyı dahil etmiştir.

Bunlar;

- Acil servisler,
- Bankacılık ve finans,
- Barajlar,
- Bilgi teknolojisi,
- Enerji,
- Hükümet tesisleri,
- İletişim,
- Kimya,
- Kritik üretim,
- Nükleer reaktörler, maddeler ve atıklar,
- Posta ve nakliye,
- Sağlık hizmeti ve kamu sağlığı,
- Savunma sanayi,
- Su,
- Tarım ve gıda,
- Ticari tesisler,
- Ulaşım sistemleri,
- Ulusal anıtlar ve simgeler

olmak üzere sıralanmaktadır.

Öte yandan Avrupa Birliğine baktığımız zaman, Avrupa Birliği Konseyi toplamda 11 adet ana başlık altında kritik altyapılarını belirlemiştir. Bunlar ise;

- Bilgi ve iletişim,
- Enerji,
- Finans,
- Gıda,
- Kamu düzeni ve güvenlik,
- Nükleer, biyolojik, kimyasal, radyoaktif madde endüstrileri,
- Sağlık,
- Sivil yönetim,
- Su,
- Ulaşım,
- Uzay araştırmaları

şeklinde sıralanabilmektedir [11]. Bu 11 ana başlık altında toplanmış olan kritik altyapılar kendi içlerinde alt başlıklara ayrılmıştır ve bu kırınımlar ile birlikte toplamda 37 adet kritik altyapı olduğu söylenebilmektedir.

Erken yıllarda kritik altyapılarını tanımlayarak, bir eylem planı oluşturan ülkelerden biri de Japonya'dır. 2005 yılından itibaren konu ile ilgili çalışmalar yürüterek politikalar oluşturmuş ve 2022 yılında son revizyon ile eylem planını yayımlamıştır [12]. "Kritik Altyapıların Korunması İçin Siber Güvenlik Politikası"nda 14 sektör kritik altyapı olarak tanımlanmıştır [13]. Bu sektörler;

- Bilgi ve haberleşme,
- Sağlık,
- Petrol endüstrileri,
- Demiryolu,
- Finans,
- Gaz,
- Elektrik,
- Havacılık
- Havalimanı
- Kredi kartı
- Kimyasal endüstrileri,
- Devlet ve yönetim
- Lojistik
- Su sektörleridir.

Türkiye'de; Afet ve Acil Durum Yönetimi Başkanlığı (AFAD) tarafından Eylül 2014 tarihinde, "2014-2023 Teknolojik Afetler Yol Haritası Belgesi" yayımlanmıştır. Bu belgenin 4.sayfasında kritik altyapıların; işlevini yerine getiremediğinde çevrede, kamuda ve toplumda önemli etkiler meydana getirecek varlıklar ve sistemler olduğu belirtilmiştir.

Bununla beraber Ulusal Siber Güvenlik Stratejisi ve Eylem Planı'nda da yine kritik altyapı tanımlamasına verilmiştir. Burada da bilginin üç temel unsurunun deforme olması durumunda, can kaybından ekonomik kayıplara ve kamu düzeninde aksamalara neden olabilecek bilişim sistemlerini barındıran yapıların kritik altyapı olarak ifade edildiğine dair açıklamalarda bulunulmuştur. Ulusal Siber Güvenlik Stratejisi ve Eylem Planında

ülkemizdeki kritik altyapıların neler olduğuna da değinilmiştir. Türkiye'de toplamda 6 adet kritik altyapı sektörü belirlenmiştir. Bunlar;

- Elektronik haberleşme,
- Enerji
- Bankacılık ve Finans
- Kritik kamu hizmetleri
- Ulaştırma
- Su yönetimi

olmak üzere sıralanmaktadırlar.

Daha önce bahsedilen ABD, AB ve Japonya tarafınca kendileri için tanımlamış oldukları kritik altyapı sektörleri ve ülkemiz için belirlenen kritik altyapı sektörlerinde ortak paydada buluşulduğu görülmektedir.

2.3. Endüstriyel Kontrol Sistemleri

Operasyonel Teknoloji (OT) sistemler, fiziksel ortamla doğrudan veya bir cihaz aracılığı ile irtibata geçen, izleyerek ya da kontrol altında tutarak süreçler üzerinde hakimiyet kurup olayları tespit eden sistem ve cihazları tanımlamaktadır [14]. Endüstriyel kontrol sistemleri (EKS) de OT sistemlerin temelini oluşturmakta olan bir parçasıdır.

EKS; çeşitli endüstriyel iş alanları ve çalışmalarda parametrelere yönelik kontrol, iş süreçlerinin yürütülmesi ve otomasyonunu sağlayan, temel olarak bilgi sistemleri kapsamında değerlendirilebilen elektronik cihazların oluşturduğu sistemlerdir [15].

Bu sistemler genellikle kritik altyapı sektörlerinde kullanılmaktadırlar. Dolayısıyla EKS'nin işlevini yitirdiği ya da çalışmasının kesintiye uğradığı durumlarda çok ciddi sorunlar ile karşı karşıya kalınma ihtimali bulunmaktadır.

Daha önce ifade edildiği gibi bilgi güvenliğinin temel unsurlarının öncelikleri, kuruluşların yapısına ve süreçlerine göre değişiklik gösterebilmektedir. EKS için en önemli unsurun, bilgiye ve hizmete kesintisiz ulaşımın sürekli hale getirilmesinin elzem olmasından dolayı, erişilebilirlik olduğu düşünülmektedir.

EKS bünyesinde "*Supervisory Control and Data Acquisition*" (SCADA), "*Main Terminal Unit*" (MTU), "*Remote Terminal Unit*" (RTU), "*Distributed Control System*" (DCS) ve "*Programmable Logic Controller*" (PLC) gibi çeşitli alt sistemler barındırmaktadır.

SCADA'nın baş harflerini alarak oluşturulduğu açılımı Türkçeye "Merkezi Kontrol ve Veri Toplama Sistemi" olarak çevrilmektedir. Kritik altyapılar sektörlerinde sıklıkla karşılaşılan SCADA sistemleri, kritik altyapılardan biri olan enerji sektöründe de elektrik üretimi ve nakil hatları, doğal gaz dağıtım ve petrol boru hatları gibi birçok alanda kullanılmaktadır [15]. Bu sistemler saha bilgilerinin toplanmasının ardından merkez üniteye iletilmesi ile operatöre neredeyse gerçek zamanlı bir izleme ve kontrol imkânı sağlamaktadırlar [14]. Sistemin bu şekilde yürütülebilmesi için MTU, RTU ve haberleşme sistemi gibi başka alt sistemlere ihtiyaç duymaktadır.

Bahsi geçen alt sistemlerden biri olan RTU yani uzak terminal birimi; saha donanımlarından elde edilen verileri izleyerek topladıktan sonra gerekliyse merkeze iletmektedir. Bir elektrik tesisi için bu verilere akım, gerilim ya da güç gibi parametreler örnektir. RTU'ların veri toplamanın yanında veri depolama, arıza tespiti ya da kumanda kontrol gibi görevleri de bulunmaktadır. Örneğin uzaktan kontrol edilen bir elektrik santralinde kesicileri açma ya da kapama komutunu gerçekleştirmektedir. Bu sistemler uzak terminal üniteleri isminden anlaşılabileceği üzere kablo ihtiyacı duymaksızın geniş bir sahada haberleşmeye elverişli oldukları bilinmektedir.

SCADA sistemleri için gerekli olan alt sistemlerden bir diğeri ise MTU yani merkezi terminal ünitesidir. MTU için kontrol merkezi de denilebilmektedir. Daha önce verilen kesici örneğinde RTU'nun bu işlemi yapabilmesi için MTU'nun komut vermesi gerekmektedir. Yönetme ve yetki verme işlemlerini yapan birim MTU olduğu için, sistemin güvenilirliğinden de sorumlu olan birimin MTU olduğu sonucu çıkartılabilmektedir [16].

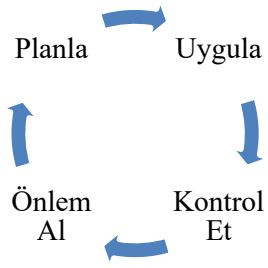
EKS'nin alt sistemlerinden olan DCS yani açılımının Türkçeye çevrilmiş hali ile dağıtılmış kontrol sistemleri, bir tesisteki süreçlerin kontrolünü birden fazla noktadan sağlayabilmekte olan dijital bir otomasyon sistemidir [17]. Enerji sektöründe petrol rafinerileri, elektrik üretimi gibi alanlarda coğrafi olarak aynı konumda bulunan sistemlerin kontrolünde örneklerine rastlanmaktadır [14]. SCADA ile benzerliklerinin yanı sıra çeşitli farklılıkları da bulunmaktadır. Daha geniş alanlar için kullanılan SCADA sistemleri eş zamanlı veri toplanması ve iletimi üzerinde yoğunlaşmışken, daha küçük çaplı alanlarda kullanılan DCS'ler süreç kontrolü üzerine yoğunlaşmışlardır [15].

PLC yani programlanabilen mantık denetleyicileri; mantık, giriş çıkış kontrolü, zamanlama ve sayma gibi fonksiyonların, geri besleme yoluyla yönetilen süreçlerde kullanılmak üzere, kullanıcı tarafından programlanabildiği bir belleğe sahip olan denetleyicilerdir [14]. Çalışma prensibi açısından RTU'lar ile ortak özellikleri bulunmaktadır.

2.4. Bilgi Güvenliği Yönetim Sistemleri

Bilgi güvenliğinin korunmasında teknoloji ile birlikte insan ve süreç faktörlerinin de önemli rol oynamaktadır [18]. Bu doğrultuda bilgi güvenliği için sacayağı benzetmesi yapılabilmektedir. Üç ayağı bulunan bilgi güvenliğinin hangi ayağında aksaklık olursa olsun çöküşe sebep olacaktır. Dolayısıyla kurumsal bilgi güvenliğinin sağlanmasında yalnızca teknik veya teknolojik tedbirler yetersiz kalacak, insan faktörünün ele alınması ve süreçlerin değerlendirilmeye katılması gerekecektir [19].

Kurumsal bilgi güvenliğinin ve bilgi güvenliği sürecinin devamlılığının sağlanması için Bilgi Güvenliği Yönetim Sisteminin yani kısaca BGYS'nin kurulması ve yürütülmesi gerekmektedir. BGYS; bilgi güvenliğinin temel unsurlarını yöneten, üst yönetimin desteğini ve kabulünü almış, bilgi güvenliği kapsamında uluslararası standartlara uygun şekillendirilmiş bir sistem olarak tanımlanabilmektedir. Bu sistem; "PUKÖ Döngüsü" ismi verilen bir modellemeye dayanmaktadır [20] . Bahsi geçen döngü, Şekil 2.4.1' de gösterilmektedir.



Şekil 2.4.1. PUKÖ Döngüsü

"Planlama" aşaması; BGYS'nin kapsamının, hedef ve amaçlarının, politikalarının, prosedürlerinin ve risklerin belirlenmesini tanımlamaktadır. Bu aşama BGYS'nin kurulması yani bu sistem için ne yapılacağına karar verilmesi olarak da ifade edilebilmektedir.

"Uygulama" aşaması; BGYS kurulurken planlanan süreçlerin ve hazırlanan dokümanların takibini, BGYS'nin işletilmesini ifade etmektedir.

“Kontrol Et” aşamasında BGYS’nin performansının değerlendirilmesi gerekmektedir. Sistemin işleyişine dair gerekli ölçümlerin yapılması ve denetim çıktıları da dahil tüm değerlendirme sonuçlarının raporlanması da bu aşamaya dahildir. Bu aşama; BGYS’nin izlenerek gözden geçirilmesi şeklinde de tanımlanabilmektedir.

“Önlem Al” aşamasında ise gözden geçirme çıktılarına dayanarak gerekli görülen düzenleyici, önleyici ve iyileştirici faaliyetlerin gerçekleştirilmesidir. Böylece BGYS’nin geliştirilmesi de sağlanmaktadır.

Bu aşamadan sonra işlemler tekrarlanmak suretiyle, döngünün yürütülmesi gerekmektedir. Sisteme, bitiş tarihi atanmış bir iş süreci ya da proje gözüyle bakılmaması gerekmektedir [21]. BGYS her zaman sürekliliğinin korunması gereken bir süreçtir. Bu yüzden sistemin sorunsuz yürütülebilmesi için PUKÖ döngüsün sağlanması önem arz etmektedir.

BGYS’nin sağlıklı şekilde yürütülmesindeki bir diğer etkenin de üst yönetimin sisteme bakış açısı olduğu bilinmektedir. Üst yönetim tarafından sağlanan destek sonucunda kurumun; BGYS ekibinin ve her birimden görevlendirilmiş BGYS sorumlularının sürecin yürütülmesini sağlaması gerekmektedir.

Kurumlarda BGYS faaliyetlerinin, bilgi güvenliğinin temel unsurlarını sağlayarak korunmasından başka yararları da bulunmaktadır. Bunlardan biri güven ortamının oluşması ile kurumsal prestijin sağlanmasıdır. Kurumla herhangi bir şekilde bağı olan insanların kişisel verilerinin korunmasının güvence altına alması ve bilgi kaynaklarına erişimin kontrol altında tutulması da BGYS’nin faydalarındandır. Bir diğer faydası ise iş sürekliliğini sağlaması, tehdit ve risklere karşı iş süreçlerinin devamlılığını garanti etmesidir. Bununla birlikte risk yönetiminin sağlanarak felaket senaryolarına karşı hazırlıklı olunmasının sağlanması da BGYS’nin faydalarından bir diğeridir.

BGYS belgelendirmeye dayanan bir sistemdir ve ülkemizde yaygın olarak tercih edilen uluslararası belge; ISO/IEC 27001 standardı belgesidir. Çalışmanın ilerleyen bölümlerinde bu hususta ki standartlar ve belgelendirme çalışmaları hakkında detaylı bilgi verilmektedir.

3. ENERJİ SEKTÖRÜ İÇİN BİLGİ GÜVENLİĞİ YÖNETİM SİSTEMİNİN ÖNEMİ

Güvenlik kavramı yıllar içinde farklı boyutlar kazanarak, kurumların hem fiziksel ortamlarda hem de siber ortamdaki saldırılara karşı duruşunun ön plana çıkmasında rol oynamıştır. Gerçek dünyada kurum ve kuruluşların, fiziksel güvenliğinin sağlanması için alınan sıkı güvenlik önlemleri bilgi güvenliğini korumak için de işe yarar durumdadır. Hem kurum personelinin hem de kuruma gelen ziyaretçilerin, kurum sınırlarına adım attığı andan itibaren uyması gereken kuralların belirlenmesi gerekmektedir. Örneğin; ziyaretçilerin hangi kapıdan giriş yaptığı, tam olarak nereye gideceği, beyan ettiği bilgilerin doğruluğu ve benzeri hususların takip edilerek gerekli önlemlerle kontrol altında tutulması ile birlikte, bilgi güvenliğinin en zayıf halkası olan insanın oluşturacağı zafiyetlerin azaltılması için bir adım atılmış olacaktır.

Bu ifadelerden bilgi güvenliğini sağlayarak kurumsal bilgileri korumanın sadece kurum sınırları içerisinde mecburi olduğu anlamı çıkartılmamalıdır. Çünkü sanal dünyada sınır söz konusu değildir. Sanal ağlarda saklanan kurumsal bilgilere uzaktan erişim sağlanması mümkün olduğu için, ilgili bilgilerin koruma altına alınması konusunda da kurallar ve önlemler belirlenmelidir. Bununla birlikte kurumsal bilgilerin harici bellekle kurum dışına çıkartılmasıyla birlikte, mobil cihazlar konusunda uyulması gereken kurallar ve alınacak önlemler kurumun fiziksel sınırlarının dışına çıkmış olacaktır.

Elbette ki dikkat edilmesi gereken birçok hususun belirlenmesi, kararlaştırılması ve ilgili kuralların yazılı olarak duyurulup saklanması kurum ve kuruluşlarda, bilginin korunması için gereken ilgili kontrollerin yapılmasını kolaylaştıracaktır. Burada Bilgi Güvenliği Yönetim Sistemi (BGYS) devreye girmektedir. Bilgi güvenliği kapsamında politika, prosedür ve talimatlarının oluşturulması, öncelikle insan kaynaklı oluşabilecek açıklıkların önüne geçmeyi hedeflemektedir. Sürekli iyileştirmeler gerektiren ve kendini güncellemeye ihtiyaç duyan bilgi güvenliği yönetim sistemi, kurum içinden veya dışından gelen her türlü saldırıya karşı önlem almayı ve her türlü zafiyeti en az seviyeye indirmeyi amaçlamaktadır. Hem kurumsal bilginin ve bilgi güvenliğinin sürekliliğinin hem de bilgi güvenliğinin üç temel unsuru olan gizlilik, bütünlük ve erişilebilirliğin sağlanmasının belgelendirme sorumluluğunu BGYS üstlenmektedir.

Kritik altyapılar için bilgi güvenliğine yönelik saldırılar, diğer tüm sektörlere göre daha fazla tehlike arz etmektedir. Bu saldırıların önlenmesi için alınan tedbirlerin açıklık bırakmadan

uygulanması, diğer bir deyişle bilgi güvenliği yönetim sistemlerinin tüm çarklarının eş güdümlü olarak dönmesi gerekmektir. Basit hatalardan oluşan zafiyetlerin geri dönüşünün olmadığı bilincinin herkesçe kabul edilebilmesi için farkındalık oluşturma çabalarının etkin hale getirilmesi gerekmektedir.

3.1. Enerji Sektörü

Enerji kaynakları ve doğal kaynaklar tarihin ilk dönemlerinden itibaren insanlığın gözde varlıklarından olmuşlardır. Uğrunda savaşlar gerçekleştirilen enerji kaynakları ve doğal kaynaklar, devletlerin zenginliği ile birlikte prestijinin anahtarı niteliği taşımaktadır.

Enerji kaynakları çeşitli yöntemlerle sınıflandırılabilmektedir. Kullanışlarına göre sınıflandırılırken yenilenebilir ya da yenilenemez olmak üzere iki kategori altında toplanan enerji kaynakları değiştirilebilirliklerine göre sınıflandırıldığında primer yani birincil ya da sekonder yani ikincil enerji kaynağı olarak belirlenmiş olan kategorilere göre ayrılmaktadırlar. Birincil enerji kaynakları; petrol, doğal gaz, kömür, biyokütle, nükleer, hidrolik, güneş, rüzgâr ve okyanus olmak üzere sıralanmaktadır. İkincil enerji kaynakları ise birincil enerji kaynaklarından türetilmiş olan elektrik, benzin, LPG (likit petrol gazı) gibi kaynaklardır.

Türkiye Cumhuriyeti Enerji ve Tabii Kaynaklar Bakanlığı (ETKB); enerji kaynakları ve tabii kaynaklardan birbiri ile ilişkili olanlarının tek çatı altında toplanmasını sağlamak amacı güdülerek 1963 yılında kurulmuştur. Kurum bu tarihten itibaren enerji kaynaklarının Türkiye Cumhuriyeti'ne yararı gözetilerek, enerji verimliliği ve çevre duyarlılığı kapsamında değerlendirilmesi misyonuyla yürütülmektedir [22].

Enerji ve Tabii Kaynaklar Bakanlığı'nın bağlı ve ilgili kuruluşları 2020 tarihinde Cumhurbaşkanlığı Kararnamesi'nin gerçekleştirdiği son değişiklikler ile güncel halini almıştır. ETKB bağlı kuruluşları, Maden Tetkik ve Arama Genel Müdürlüğü (MTA) ile Maden ve Petrol İşleri Genel Müdürlüğü (MAPEG) iken ilgili kuruluşları, Elektrik Üretim A.Ş. Genel Müdürlüğü (EÜAŞ), Türkiye Elektrik İletim A.Ş. Genel Müdürlüğü (TEİAŞ), Türkiye Elektrik Dağıtım A.Ş. Genel Müdürlüğü (TEDAŞ), Boru Hatları İle Petrol Taşıma A.Ş. (BOTAŞ), Türkiye Petrolleri Anonim Ortaklığı Genel Müdürlüğü (TPAO), Türkiye Kömür İşletmeleri Kurumu Genel Müdürlüğü (TKİ), Türkiye Taşkömürü Kurumu Genel Müdürlüğü (TTK), Eti Maden İşletmeleri Genel Müdürlüğü (ETİ MADEN), Türkiye

Elektromekanik Sanayi A.Ş. Genel Müdürlüğü (TEMSAN), Türkiye Enerji Nükleer ve Maden Araştırma Kurumu (TENMAK) olmak üzere kararlaştırılmıştır. Bu kuruluşların yanı sıra Enerji Piyasası Düzenleme Kurumu (EPDK) ve Nükleer Düzenleme Kurumu (NDK), ETKB ilişkili kuruluşları olarak sayılmaktadır. Bağlı ve ilgili kuruluşlar bir ya da birden fazla enerji alt sektöründe çalışmalarını yürütmektedirler. Enerji sektöründeki faaliyetleri anlayabilmek için bahsi geçen kuruluşların misyonları ve enerji sektörüne olan katkılarının bilinmesi gerekmektedir. Bu bilgiler aşağıda kuruluşların yanında kısaca açıklanmaktadır.

- MTA: 2804 Sayılı kanun ile 1935 tarihinde kurulmuş olan MTA; jeoloji ve maden alanlarında yürütülen araştırma ve analiz gibi çeşitli çalışmalar sayesinde üretilen bilgiler neticesinde ülkenin zenginliğine katkıda bulunma misyonuyla faaliyetlerini sürdürmektedir [23].
- MAPEG: 1954 yılında 6326 sayılı Kanun ile kurulan Petrol Dairesi Reisliği; 1973 yılında 1702 saylı Kanun ile T.C. Petrol İşleri Genel Müdürlüğü (PİGM) olarak isimlendirilmiş olup 2011 yılına kadar ETKB bağlı kuruluşu olarak görevlerini yürütmüştür. Bu sıra Maden İşleri Genel Müdürlüğü (MİGEM) de 1993 yılında 505 sayılı Kanun ile Maden Dairesi'nin MİGEM olarak değiştirilmesi ile kurulmuştur. 2018 yılında ise 703 sayılı kanun Hükmünde Kararname ile MİGEM ve PİGM kaldırılarak bu iki Genel Müdürlüğün görevleri birleştirilmek suretiyle; tabii kaynakların araştırılması gibi çeşitli faaliyetlerin yürütülmesi ve bu işlemler gerçekleştirilirken halkın faydasının ve ülkenin refahının gözetilerek gerçekleştirmek misyonunu taşıyan MAPEG kurulmuştur. [24]
- TEDAŞ: TEDAŞ Genel Müdürlüğü; 1970 yılında kurulmuş olan Türkiye Elektrik Kurumu (TEK) kapsamında yürütülen elektrik üretim, iletim ve dağıtım hizmetlerinin 1993 yılında Türkiye Elektrik Üretim A.Ş. (TEAŞ) ve Türkiye Elektrik Dağıtım A.Ş. (TEDAŞ) olarak ayrılması sonucu faaliyetlerine başlamıştır. Tüm çalışmalarını "Aydınlık Bir Türkiye" vizyonuyla ve elektriğin arz edildiği halkın memnuniyetini baz alarak sürekli ve kaliteli hizmetin sağlanması misyonuyla yürütmektedir [25].
- EÜAŞ: 2001 yılından itibaren faaliyet gösteren EÜAŞ Genel Müdürlüğü, elektrik enerjisinin ülkenin refahını sağlamak amacıyla kaynaklarımızın çevreye duyarlı ve en verimli şekilde kullanmak suretiyle sürekliliğin korunarak üretilmesi misyonunu taşımaktadır [26].

- TEİAŞ: 2001 yılında kurulduktan sonra, 2003 yılında Enerji Piyasası Düzenleme Kurumu (EPDK) tarafından "İletim Lisansı" kapsamında çalışmalar yürüten TEİAŞ Genel Müdürlüğü, elektriğin milli enerji politikaları ile uyumlu, çevreye duyarlı, verimli ve güvenilir şekilde tüm ülkeye iletilmesinin devamlılığını hedeflemektedir [27].
- BOTAŞ: 1974 yılından itibaren faaliyet gösteren BOTAŞ'ın kurulduğu yıllarda Türkiye Cumhuriyeti'nin Irak ile 1973 yılında imzalamış olduğu "Ham Petrol Boru Hattı Anlaşması" kapsamında ham petrolün Iraktan İskenderun Körfezi'ne taşınması amaçlanmıştır. Kuruluş her ne kadar ilk yıllarında boru hatları ile petrol taşınması üzerine faaliyet gösterse de ilerleyen yıllarda doğal gaz taşınması üzerinde de çalışmalar yürütmeye başlamıştır. Misyonu ise enerji verimliliğine ve kaliteye özen göstererek üst düzey teknolojilerin kullanımı ile enerji arzını gerçekleştirmektir. [28]
- TPAO: Türkiye'nin milli petrol şirketi olan TPAO, 1954 yılında kurulmuştur. Kuruluşunda amaç; hidrokarbon üzerine arama, sondaj, üretim, rafineri ve pazarlama alanlarında çalışmalar yürütmektir. Bu nedenle TPAO; Türkiye Cumhuriyeti'nin petrol ve doğal gaz sektörlerindeki üretimini çoğaltmak için hem yurt içinde hem de yurt dışında çeşitli çalışmalar yürütmeyi misyon edinmiştir [29].
- TKİ: Kurum, 1957 yılında kurulmuş, kurulduğu günden 1980 yılına kadar taşkömürü ve asfalt dahil kömür üretimi ve kömür sahalarından özellikle büyük çapta olanlarının devletleştirilmesi gibi faaliyetler yürütmüştür. Daha sonraki yıllarda Türkiye Taşkömürü Kurumu kurulunca, TKİ termik santrallerde kullanılan linyit alanında çalışmalarına yoğunlaşmıştır. Günümüzde devam eden kömür sektörüne yönelik etüt araştırma ve projeleri ve ar-ge projeleri bulunmaktadır. [30]
- TTK: Kuruluşu resmi olarak 1983 yılında TKİ'den ayrılan Ereğli Kömür İşletmeleri'nin genel müdürlük olarak yapılandırılmış olsa da TTK ambleminde Zonguldak bölgesindeki taşkömürü madenciliği faaliyetlerinin başladığı tarih olan 1848 yılına yer verilmiştir. Kuruluş enerji ve demir çelik sektörlerindeki metalurjik kömür ihtiyacının ülkenin refahı için güvenli ve çevreye duyarlı şekilde giderilmesinde taşkömürü rezervlerinden faydalanmak misyonuyla çalışmalarını yürütmektedir [31].
- ETİ MADEN: 1935 yılında Gazi Mustafa Kemal Atatürk'ün talimatıyla yer altı kaynaklarımızı değerlendirmek, hammadde ve enerji üretilmesini sağlamak için kurulan Etibank; 1998 yılında gerçekleştirilen ilk yapılandırma sonucu Eti Holding

A.Ş. ve ardında 2004 yılında ikinci yapılandırma ile günümüzdeki halini alarak Eti Maden İşletmeleri Genel Müdürlüğü adı altında çalışmalarını sürdürmektedir. ETİ MADEN, bor ve diğer nadir toprak elementleri gibi çeşitli maden kaynaklarının değerlendirilmesi ile ilgili yürütülen çalışmalarda yenilikçi ve sürdürülebilir bakış açısının benimsenmesi ve üretilen bilgi ile sektördeki varlığını sürdürme misyonuyla yürütülmektedir. [32]

- TEMSAN: Bakanlar Kurulu kararı ile 1975 yılında kuruluşu ile ilgili idari işlemlerin başlatıldığı TEMSAN, gerekli hazırlıklar tamamlandıktan sonra 1977 yılında faaliyetlerine başlamıştır. Kuruluş amacı hidroelektrik santraller için gerekli olan teçhizatların yerli üretim olmasının sağlanması iken günümüzde; enerji sektörü için test laboratuvarları kurup yürütmek, enerji santrallerinin her türlü ihtiyacına karşılık hizmet vermek, endüstriyel sistemler için AR-GE ve ÜR-GE faaliyetleri yürütmek gibi ülke ekonomisine katıda bulunacak çok çeşitli çalışmaları bulunmaktadır [33].
- TENMAK: Kurum 2020 yılında, Cumhurbaşkanlığı Kararnamesi ile ETKB'ye bağlı kuruluşlardan Türkiye Atom Enerjisi Kurumu, Ulusal Bor Araştırma Enstitüsü ve Nadir Toprak Elementleri Araştırma Enstitüsü' nün kapatılarak bu kuruluşların görevini kapsamına dahil etmek suretiyle kurulmuştur. Bünyesinde, Bor Araştırma Enstitüsü'nü, Nadir Toprak Elementleri Araştırma Enstitüsü'nü, Temiz Enerji Araştırma Enstitüsü'nü, Nükleer Enerji Araştırma Enstitüsü'nü ve Enerji Araştırma Enstitüsü'nü barındıran TENMAK bu alanlarda çeşitli faaliyetler yürütmektedir. [34]

Geçmişten günümüze kadar dünya üzerinde kritik altyapılara yönelik sayısız saldırı meydana gelmiş, bunların bir kısmı önlenememiş veya engellenememiştir. Enerji sektörü de çalışma alanları dolayısıyla siber saldırılara oldukça açık bir sektördür.

Enerji ve Tabii Kaynaklar Bakanlığı'na yönelik günlük 500 bin civarı siber saldırı Bakanlık tarafından tespit edilerek, önlenmektedir. Bu çalışmalar bilgi güvenliği yönetim sistemine entegre şekilde gerçekleştirilmektedir.

3.2. Siber Saldırı Yöntemleri

Bu bölümde siber saldırı yöntemlerinden en bilindik olanları ile ilgili bazı açıklamalara yer verilmiştir.

3.2.1. Kötücül yazılımlar

Bilgisayar sistemlerine zarar vermeyi hedefleyerek sistem bilgilerine erişmeye çalışan, kötü amaçlı bilgisayar programlarına *malware* denmektedir. Malware kelimesi "*malicious software*" yani kötücül yazılım ifadesinin kısaltılmış halidir.

Malware kapsamına çeşitli yazılımlar bulunmaktadır. Bunlardan en çok bilinenleri virüsler, solucanlar, Truva atları (*trojan*), casus yazılımlar (*spyware*), fidye yazılımlar (*ransomware*) ve mantık bombalarıdır (*logic bomb*) [35]

Virüsler; kendiliğinden çoğalabilen ve kendinin neredeyse birebir kopyalarını birtakım yollarla başka bilişim sistemlerine göndererek yayılan yazılımlardır. Virüs terimi ilk olarak Fred Cohen isimli öğrencinin tezinde kendine yer bulmuştur. Cohen, virüslerin kendi kendini kopyalayabilmesinden ötürü, tez danışmanının önerisiyle, tezinde bu terimi kullanmıştır. Virüsler kullanıcı tarafından çalıştırılmak suretiyle etkin hale gelmekte ve genellikle mail veya USB yoluyla meydana gelebilmektedir [35].

Truva atları; ismini Truva savaşı esnasında gerçekleştirilen meşhur şaşırtmacadan almaktadır. Çalışma prensibi yararlı olduğu zannedilen bir programın arka planında çalışmasına dayanır. Bu şekilde bilişim sistemlerine bulaşan Truva atları, kişinin iradesi dışında faaliyet göstermektedir. Virüslerden farklı olarak kendiliğinden çoğalma özelliği yoktur ve kendisine tanımlanmış görev ne ise onu gerçekleştirmektedir. Karakteristik özelliği olarak sızdıkları bilişim sistemlerinin uzaktan izlenip, kontrol edilmesi ve veri aktarımı sağlaması olduğu bilinmektedir [35]. En bilinen örneklerinden biri "TrickBot malware" adı verilen; finansal verileri çalmak amacıyla geliştirildikten sonra çeşitli siber suç faaliyetleri gerçekleştirerek çok katmanlı bir hale dönüşen bir kötücül yazılımdır [36].

Solucanlar; sıklıkla karıştırıldıkları virüslere benzer şekilde kendini bir bilişim sisteminden bir başka bilişim sistemine kopyalamak için yaratılmış kötücül yazılımdır [35]. Solucanların virüslere benzerlik taşıyan yönleri olduğu gibi farklı yönleri de bulunmaktadır. Virüslerden farklı olarak ağ üzerinden otomatik olarak yayılmakta, kullanıcının çalıştırmasına ihtiyaç duymamaktadır. Ulaştıkları bilişim sisteminin güvenlik duvarını aştıktan sonra virüse benzer

şekilde hareket edip sistemi enfekte edebilmekte veya Truva atına benzer şekilde hareket ederek gizli bilgileri bir başka yere aktarabilmektedir. En bilinen örneklerinden biri ciddi miktarda maddi kayba da sebep olan "ILOVEYOU" adı verilen solucandır.

Mantık bombaları; tetiklenmeye dayanan bir zararlı yazılım çeşididir. Mantık bombaları aktive olana kadar sızdığı bilişim sistemine zarar vermeden beklemektedir. Aktive olması için daha önce belirlenmiş bir zamanın gelmesi ya da özel durumun gerçekleşmesi gerekmektedir. Gerçek yüzünü gösterdikten sonra bilişim sistemine çeşitli zararlar verebilmektedir. Mantık bombalarının en meşhur örneklerinden biri Çernobil (CIH) Virüsüdür. Bilinen farklı versiyonları olan virüsün versiyonlarından biri her yıl 26 Nisan'da yani Çernobil faciasının gerçekleştiği günde faaliyete geçerken bir diğer versiyonu her ayın 26.gününde faaliyete geçmektedir [37].

Spyware yani casus yazılımlar; adından anlaşılabileceği üzere bilişim sistemlerinde casusluk yapması için oluşturulmuş kullanıcının bilgisi olmadan yüklenen yazılımlardır. Casus yazılımlar virüs ve solucanlar gibi bilişim sistemine bulaştıktan sonra yayılma ihtiyacı duymamaktadırlar çünkü bulaştıkları bilişim sisteminde gizlenerek bilgilerin toplanmasını sağlamaktır [35]. Bu yazılımlar potansiyel saldırgana aktarmak üzere, kullanıcının klavye vurgularından banka hesapları gibi kritik noktalarda kullandığı her türlü parolasına kadar çeşitli kişisel bilgilerini kaydedebilmektedir. En bilindik casus yazılımlardan bir tanesi "keylogger" adı verilen yazılımdır. Keylogger'ın temel mantığı klavyede yapılan her hareketin kaydedilmesi üzerine kurulmuştur [38].

Ransomware yani fidye yazılımların temel hedefi Truva atı gibi çeşitli kötücül yazılımlar yardımı ile bilişim sistemine sızdıktan sonra sistemi kilitleyerek kullanıcıdan para talep edip kazanç sağlamaktır. Bu süreç bazı aşamaları içermektedir. Bu süreç öncelikle bilişim sistemine sızılarak kontrol altına alınması, ardından sistemin şifrelemesi ya da kilitlenmesi yoluyla kurbanın sistem üzerindeki verilerine erişiminin engellenmesinin sağlanması, daha sonra kurbana fidye miktarının ve fidyeyi nasıl ödeyeceğinin bildirilmesi, bunun ardından kurbanın ödeme yapması ve ödemenin saldırgana ulaştığının kontrolünün sağlanması ve son olarak fidyenin ödenmesinin ardından saldırgan tarafından kilidin kaldırılmasıyla kurbanın tekrar verilerine erişim sağlaması adımları ile gerçekleşmektedir [39].

3.2.2. Phishing (oltalama) saldırıları

Phishing yani oltalama saldırısı; kişiyi kendisine gelen e-mail veya mesajın güvenilir bir kaynaktan gönderildiğine inandırmak suretiyle kandırmaya yönelik gerçekleştirilen saldırı türüdür. Phishing kelimesi; İngilizcede şifre anlamına gelen *password* kelimesiyle balık tutmak anlamına gelen *fishing* kelimesinin birleştirilmesinden oluşmuştur. Temel amacı kurbanın banka hesabı, kimlik numarası, çeşitli şifreler gibi kişisel bilgilerinin ele geçirilmesidir. Sosyal mühendisliğin en çok tercih edilen saldırı formlarından biri olan phishing; saldırgan tarafından küçük veya büyük maddi kayıplara sebep olabilmektedir. Saldırılar; e-mail veya mesaj ile gönderilen güvenli gibi gösterilmiş bir bağlantıya tıklanması hususunda talimatlarda bulunup ardından kullanıcıyı yasal olmayan bir siteye yönlendirerek bilişim sistemine malware yüklenmesine sebep olacak ya da kullanıcıya inandırıcı bir ekran üzerinden kimlik bilgilerini ve şifresini girmesini isteyerek bu bilgilerin saldırganın eline geçmesine olanak sağlayacak şekilde gerçekleşebilmektedir [40].

Bu tür saldırıların sebep olacağı kayıpların azaltılması için en önemli husus farkındalık oluşturmaktır. Atalarımızın "bir musibet bin nasihatten evladır" yaklaşımından yola çıkarak kurumlarda BGYS kapsamında phishing benzeri sosyal mühendislik tatbikatları yapılmaktadır.

3.2.3. DOS ve DDOS saldırıları

DOS (*Denial of Service*) yani "servis hizmeti reddi" saldırıları bir kaynaktan sistemin kaldırabileceğinden fazla ağ trafiğine sebep olacak şekilde yüklenmesiyle, kullanıcının sisteme erişiminin kesintiye uğramasına ya da sistemin tamamen çökmesine sebep olan türde saldırılardır [41]. DDOS (Distributed Denial of Service) yani "dağıtılmış hizmet reddi" saldırıları da DOS saldırılarına benzer çalışma prensibi içeren ancak tek bir kaynaktan değil de birden fazla kaynaktan saldırının başlatılmasıyla gerçekleştirilen saldırı türüdür. Bu işlemin gerçekleştirilmesi için, saldırganlar genellikle virüsü gönderdikleri bilişim sistemlerinden oluşan bir botnet (zombi ağı) kullanmaktadırlar [42].

Bu tür saldırıların önlenmesinin zor olmasının sebebi kötücül bir trafik isteği ile meşru bir trafik isteğinin aynı portu ve protokolü kullanmaları sebebiyle birbirinden ayrılamamasıdır [40]. Saldırganların DDOS saldırılarını gerçekleştirebilmek için tercih ettiği; "volüm tabanlı

saldırılar", "protokol tabanlı saldırılar" ve "uygulama katmanı saldırılar" olmak üzere üç kategoride çeşitli yöntemler olduğu bilinmektedir [43].

3.2.4. Man in the middle (MITM) saldırıları

*Man in the middle (*ortadaki adam) ya da kısaca MITM saldırıları; istemci ve sunucu arasındaki iletişimin arasına girilerek dinlenmesi, istemci ya da sunucu gibi davranarak veri hırsızlığı yapılması ya da iletişimin değiştirilmesi şeklinde gerçekleşebilmektedir [40]. Bu tür saldırıların en bilinen örneği Wi-Fi ağlarının kullanılması ile gerçekleşmektedir. Kullanıcının halka açık bir Wi-Fi ağına bağlanmasının ardından saldırganın devreye girerek, kullanıcının kişisel verilerini ele geçirebilmektedir.

3.2.5. SQL (*structured query language*) enjeksiyonu

SQL (yapılandırılmış sorgu dili) bir web uygulamasının veri tabanında; veri bulma, veri özetleme veya otomatik görev oluşturma gibi sorgulamaları ve işlemleri yapan bir dildir [44].

Enjeksiyon saldırılarından biri olan SQL *injection* (enjeksiyon) saldırıları; saldırganın veri tabanına erişebilmesini sağlamaya yönelik SQL'in karakteristiğinden yararlanarak gerçekleştirilen bir saldırı türüdür [45]. Saldırgan SQL komutlarını veri tabanında yetkisi olmadan çalıştırarak, o veri tabanının mimarisini çözümlemeyi hedeflemektedir. Bu çalıştırma işlemi standart bir SQL sorgusunun değiştirilmesiyle ya da SQL komutlarını değiştirmek amacıyla yanlış filtrelenmiş karakterlerin kullanılmasıyla gerçekleştirilebilmektedir [40].

SQL enjeksiyonu saldırıları örneğine ülkemizde 2013 yılında "RedHack" isimli hacker grubunun Diyanet İşleri Başkanlığı'nın web sitesinin veri tabanına girmesiyle rastlanmıştır [45].

3.2.6. Password saldırıları

Password (şifre) saldırıları; bilişim sistemlerinde saklanan şifreleri illegal yollarla elde etmek üzerine tasarlanmış saldırılardır. Saldırgan kullanıcının şifresini ele geçirmek için çeşitli yöntemler uygulayabilmektedir. Bu yöntemlerin başında Türkçeye kaba kuvvet

olarak çevrilmiş *brute force* saldırıları gelmektedir. Tüm kombinasyonları ihtimal dahilinde deneyerek şifrenin kırılmasını sağlamak amaçlanırken ilk olarak en basit parolalar tahmin edilmektedir. Bir diğer yöntem olan *dictionary* (sözlük) saldırılarında ise brute force saldırılarından farklı olarak tüm parolalar değil, doğru olma ihtimali yüksek olanlar tahmin edilerek denenmektedir. En çok uygulanan yöntemlerden bir diğeri ise *password spraying* yani parola püskürtme saldırılarıdır. Bu saldırılarda ise, saldırgan en çok kullanılan parola kombinasyonlarını deneyerek kullanıcının şifresini kırmayı amaçlamaktadır.

Şifre saldırılarının yol açacağı tahribatların büyüklüğü düşünüldüğünde, bu durumdan kaçınmak için bazı önlemlerin alınması tavsiye edilmektedir. Karmaşık şifrelerin kullanılmasının bu tip saldırıları önleyebileceği bilinmektedir. Kurum ve kuruluşlarda BGYS kapsamında parola politikaları oluşturularak; kullanıcıya parolalarını belirlemek için çeşitli yönergelerde bulunulmakta ve kullanıcıların düzenli aralıklarla parolalarını değiştirmeleri istenmektedir.

3.3. Global Çerçevede Enerji Sektöründe Gerçekleşen Siber Saldırılardan Bazıları

Gerekli tedbirlerin alınmasına karşın enerji sektörüne yönelik gerçekleşmiş başarıyla sonuçlanan çok sayıda saldırı bulunmaktadır ve bu saldırılar büyük tahribatlar meydana getirmiştir. Üst düzey teknolojilerin kullanılması saldırının başarısız olacağı garantisini vermemektedir. Daha önce de ifade edildiği gibi bilgi güvenliğinin en zayıf halkası olan insanı hedef alan saldırıların başarıya ulaşma ihtimalinin daha yüksek olduğu gözlenmiştir. Sosyal mühendislik ile gerçekleştirilen saldırılara karşı alınabilecek yegâne önlem kişilerin farkındalıklarını arttırmaya yönelik çalışmalardır. ISO/IEC 27001 standardı gibi bilgi güvenliği standartlarında farkındalık eğitimlerinin belirli periyotlarla gerçekleştirilmesi mecburi tutulmuştur. Bu husus da bizi yine başarılı şekilde kurulmuş ve iyi şekilde yürütülen bir Bilgi Güvenliği Yönetim Sistemine yönelik doğan ihtiyaca ulaştırmaktadır.

Enerji sektöründe gerçekleştirilen saldırıların birçoğunun insandan kaynaklanan zafiyetler sebebiyle gerçekleştirildiği bilinmektedir. Tedbir alınmamış, görmezden gelinmiş ya da önemsenmemiş risklerin veya risk olarak tanımlanmamış bazı tehditlerin de saldırıların başarıyla sonuçlanmasına sebep olabilmektedir.

Bu bölümde enerji sektörüne karşı gerçekleştirilen saldırılardan hem kamuoyunda ilgi uyandırmış hem de ülkelerini ve/veya kuruluşlarını büyük zarara uğratmış olanlarından bazıları hakkında bilgi verilmektedir.

3.3.1. Sibirya'da doğalgaz boru hattı patlaması

1982 tarihinde siber teknolojiden faydalanarak meydana getirilmiş ilk saldırı olan ve neredeyse bir nükleer patlamaya eşdeğer şiddette gerçekleşmiş olan bu doğalgaz boru hattı patlaması, ilk siber saldırı olarak bilinmesinin yanı sıra nükleer patlamalar haricinde uzaydan görülebilen en büyük patlamalardan biri oluşuyla bilinmektedir [46].

The Washington Post' da yayımlanmış bir habere göre; dönemin ABD Başkanı Ronald Reagan Soğuk Savaş döneminde meydana gelen bu patlamanın CIA (*Central Intelligence Agency)* yani ABD'nin merkezi istihbarat teşkilatı tarafından uygulanan bir plan olduğunu onaylamıştır [47].

ABD'nin liderlik ettiği Batı Blok'u ülkeleri ile 1922 ve 1991 yılları arasında varlığını sürdüren Sovyet Sosyalist Cumhuriyetler Birliğinin (SSCB) liderliğindeki Doğu Blok'u ülkelerinin arasında var olduğu bilinen ve yaklaşık 45 yıl süren gerginlik 'Soğuk Savaş' olarak isimlendirilmektedir. Soğuk Savaş döneminde ABD öncülüğünde Batı Blok'unun SSCB'ye ambargo uygulamasından dolayı, SSCB'nin her türlü ihtiyacını zaman zaman illegal olmak üzere alternatif yollarla gidermeye çalıştığı bilinmektedir. Böyle bir dönemde doğalgaz boru hattında kullanılmak üzere ihtiyaç duyduğu kontrol sistemini Kanada'dan çalan SSCB, beklemedikleri bir tehditle karşı karşıya kalmıştı [48]. Çünkü ABD, SSCB'nin doğal gaz ithal etmesine engel olmaya çalışmaktaydı ve bu yüzden çalıntı kontrol sistemine CIA operasyonuyla bir mantık bombası yerleştirilmişti [47]. Doğalgaz boru hattı patlamasına, bu mantık bombasının boru hatlarında gerçekleşen akışın normal dışı değerlere yükselmesini sağlaması sebep olmuştur [46].

3.3.2. Slammer solucanı ve Davis-Besse nükleer santrali

Bu saldırı; Slammer isimli solucanın 2003 yılında ABD'nin Ohio eyaletindeki Davis-Besse nükleer santraline bulaşması ile gerçekleşmiştir [49]. Bu saldırıda doğrudan nükleer santral hedeflenmemiştir ancak yine de santral efekte olmuştur [50]. Slammer solucanı bulaştığı sistemlerde verileri silme veya değiştirme yapacak bir yük taşımamasına karşın büyük

miktarda sahte trafiğe yol açmış ve güvenlik parametrelerini görüntüleme sistemini yaklaşık dört saat elli dakika kadar erişilemez hale getirmiştir [51].

Slammer solucanının sisteme sızmasına yardımcı olan en büyük zafiyet; çalışan bir güvenlik duvarının olmasına rağmen santralin bir yüklenicisinin kendi şirket ağını doğrudan tesisin bilgi işlem sistemine bağlayan bir internet bağlantısı kurmasıyla gerçekleşmiştir [52].

3.3.3. Night Dragon

Night Dragon; McAfee isimli siber güvenlik firmasının 2009 yılında başlayan siber saldırılara verdiği isimdir [53]. Night Dragon çok yönlü sosyal mühendislik, oltalama ve Microsoft Windows işletim sistemindeki güvenlik açıklarından yararlanmak için Truva atı türlerindeki çok karışık olmayan ancak saldırganın istikrarına ve becerisine dayanan saldırıları içermektedir [54, p. 101]. Bu saldırılar; petrol ve gaz alanlarındaki şirketlerin kontrol sistemlerine ve operasyon bilgileri gibi hassas gizli verilerine ulaşıp kaydetmesi amacıyla stratejik olarak tasarlanmıştır [55]. McAfee firmasının raporuna göre; saldırganlar hedef aldıkları sistemler üzerinde tam kontrol sağlamış, eriştiklerinden daha hassas bilgilere ulaşabilmek adına bir şifre kırma aracından faydalandıkları söylenmektedir [53].

3.3.4. Stuxnet saldırısı

2008 yılında İran'daki Natanz nükleer santralindeki santrifüjlerde başlayan daha önce benzeri görülmemiş çöküşlerin 2010 yılına dek tesadüfi olduğu varsayılmıştır [51]. Oysaki Natanz nükleer santralindeki mühendislerin farkında olmadan karşı karşıya kaldığı durum 21.yüzyılın en büyük siber olaylarından biri kabul edilmektedir. Oldukça ileri seviyede bir kötücül yazılım olan Stuxnet solucanı, kendisini kopyalayabilmekte ve bu sayede ağ içerisinde derinlemesine yayılıp ağı işlevsiz hale getirebilmektedir [56].

Stuxnet öncelikle bir USB aracılığıyla yerel ağda bulunan ve motor hızına karar veren PLC'leri, ardından santrifüjlerin üzerinden geçen akımının frekansının değiştirilip makinelerin parçalanmasını hedefleyerek sistemi iki aşamada ele geçirmiştir [57]. Bu iki aşama gerçekleştirilirken merkez bilgisayarlarda herhangi bir anormallik görülmemiştir ki bu durum Stuxnet'in oldukça geç anlaşılarak tanımlanmasına sebep olmuştur [56].

Stuxnet'in; nihayet 2010 yılında Ukrayna'da bir firmanın fark edilmesi ve tanımlaması ile dünya çapında bilinen büyük siber güvenlik ve anti virüs şirketleri solucan üzerinde araştırmalar gerçekleştirmişlerdir [56]. Bütün bu araştırmaların sonucunda Stuxnet'in sıradan bir solucana göre fazlasıyla karmaşık olduğu, iyi finanse edilmiş saldırganlar

tarafından tasarlandığı sonucuna varılmış ve böylece kuvvetli şekilde desteklenen bir saldırganın arzu ettiği sisteme saldırabileceğine kanaat getirilmiştir [53].

Saldırının zararlarının tam olarak hesaplanamadığı bilinmektedir ancak saldırının gerçekleştirilmesinden sonra zarar görmüş olan 1000 adet santrifüjden 600 tanesi değiştirilmiştir [57].

3.3.5. Dragonfly grubunun saldırıları

2011 yılından itibaren faaliyet gösteren Dragonfly isimli hacker grubu, Avrupa ve Amerika'da çeşitli kritik altyapılara karşı saldırılar gerçekleştirmişlerdir [58]. Dragonfly; saldırılarını gerçekleştirmek için sızma faaliyetlerini çeşitli yöntemlerle gerçekleştirmiştir. Bu yöntemler; yöneticiler ve kıdemli çalışanların kötü amaçlı e-posta ve dosya eklerini kullanarak gerçekleştirilen kimlik avı, *watering hole* ismi verilen hedefteki kullanıcıların sık ziyaret ettiği sitelere bulaştırılan virüsler ve EKS firmalarının web sitelerinden indirilen Truva atı bulaştırılmış yazılımlar şeklinde sıralanmaktadır [59]. Grubun önceliği casusluktur. Hedefledikleri sektörler ise endüstriyel kontrol sistemleri kapsamında faaliyette bulunan petrol boru hattı operatörleri, elektrik üretim firmaları gibi enerji şirketleri ve bununla birlikte diğer kritik altyapıları olmuştur (Khan ve diğerleri, 2023).

Bir süre faaliyetlerini durduran Dragonfly'ın, 2015 yılında Drogonfly 2.0 ile tekrar aktif hale geldiği ve daha önce Türkiye'de saldırı gerçekleştiren grubun yeniden Türkiye'yi hedef aldığı bilinmektedir [60].TRT Haber'e göre İstanbul ve civarındaki büyük elektrik kesintileri bu hacker grubunun saldırıları ile ilişkilendirilmektedir [61].

3.3.6. Shamoon virüsü saldırıları

2012 yılında gerçekleşen Shamoon virüsü saldırıları birbiri takip eden 12 gün içerisinde önemli enerji şirketlerini hedeflemiştir. İlk saldırı 15 Ağustos'ta Saudi Aramco isimli petrol ve doğalgaz bazlı enerji şirketine, ikinci saldırı ise 27 Ağustos tarihinde RasGas isimli Katar merkezli LNG yani sıvılaştırılmış doğal gaz şirketine gerçekleştirilmiştir [53].

Bilişim sistemlerine bulaştıktan sonra onları kullanılamaz hale getirmeyi hedefleyen Shamoon virüsü, ilk saldırının gerçekleşmesiyle birkaç saat içinde yaklaşık 30 bin bilgisayara zarar vermiştir [46]. Her ne kadar asıl hedef olan petrol ve gaz akışının kesintiye uğratılması gerçekleştirilmese de bilgisayarlardaki birçok önemli veri silindikten sonra, resimlerin yerine yanan bir ABD bayrağı görseli bırakılmıştır [62]. Saldırının sebep olduğu zararların giderilmesi yaklaşık iki hafta sürmüş, firmanın enerji piyasasında önemli yeri olan

bir firma olması ve saldırının büyük ölçekte zarar vermesi sebebiyle ABD ve diğer birçok ülke saldırıdan kaynaklı hasarların telafi edilmesi için iş birliği yapmıştır [63].
Saldırıyı "Cutting Sword of Justice" yani "Adaletin Keskin Kılıcı" isimli hacker grubu üstlenmiştir [46].

3.3.7. Telvent firmasına saldırı

Telvent; Kanada'da yer alan, yenilenebilir enerji, petrol ve doğalgaz başta olmak üzere çeşitli projeleri bulunan ve Kuzey Amerika'nın petrol ve gaz pazarının yarısına yakın bir kısmını domine eden bir firma olmasıyla tanınmaktadır [64]. Firma; 10 Eylül 2012 tarihinde, güvenlik ağlarının ihlal edildiğini bildirmiştir [65]. Saldırganlar Truva atı kullanarak firma ağına sızdıktan sonra projelere ve müşterilere ait bilgileri ele geçirmişlerdir.

3.3.8. Güney Kore nükleer santral saldırısı

Özellikle 2013 ve 2016 yılları arasında; Kore Demokratik Halk Cumhuriyeti ya da daha yaygın ismiyle Kuzey Kore'nin, Güney Kore ya da resmi ismiyle Kore Cumhuriyeti'ne yönelik çeşitli siber saldırılarda bulunduğu iddia edilmektedir.
Bu saldırılardan en önemlilerinden biri olanı; 2014 yılında "Kore Hidro ve Nükleer Güç Şirketi"ne gerçekleştirilmiştir. Saldırının ilk aşaması phishing mailleriyle başlatılmıştır. Şirket personellerine atılan maillerle şirketin iç ağına yerleşen kötücül yazılımlar yayılmıştır. Bunun sonucunda şirkete ait çeşitli bilgiler ele geçirilmiştir.
Bu aşamadan sonra saldırganlar sosyal medya üzerinden çeşitli mesajlar yayınlayarak, şirketin 3 reaktörünü Noel'e kadar kapatmadığı sürece daha fazla verisini ifşa etmekle tehdit etmişlerdir [66].
Saldırıların komut ve kontrol sunucusu (C2 sunucusu) kullanılarak gerçekleştirilmesi sebebiyle, bu yöntemi benimseyen hacker grubu Kimsuky veya DarkHotel'in gerçekleştirdiği düşünülmektedir [67].

3.3.9. BlackEnergy

23 Aralık 2015 tarihinde Ukrayna'da enerji dağıtım şirketlerine yönelik gerçekleşmiş ve altı saat sürmüş olan elektrik kesintisi yüz binlerce kişinin elektriksiz kalmasına sebep olmuştur.

“BlackEnergy” ismindeki Truva atı; DDOS saldırısı ve sosyal mühendislik gibi saldırı yöntemleriyle yalnızca Ukrayna’da değil, dünya çapında endüstriyel kontrol sistemlerini hedef alarak saldırılar gerçekleştirmiştir [68].

Ukrayna’da meydana gelen saldırıda ilk olarak hedef alınan şirketin çalışanlarına yönelik phishing mailleri atılmış, şirket ağına sızma işlemi gerçekleştirildikten sonra 30 adet trafo merkezinde elektrik kesintileri yaşanmıştır [69].

ABD; Rusya’nın yıllardır Ukrayna’nın kritik altyapılarına karşı yürüttüğü sistematik kampanyadan ötürü, bu saldırıdan da Rusya’nın sorumlu olduğuna dair iddialarda bulunmaktadır [70].

4. BİLGİ GÜVENLİĞİ YÖNETİM SİSTEMİ İÇİN YOL HARİTALARI

TDK'ya göre standart kavramı "belirli ölçülere, yasaya, kullanıma uygun olan" olarak tanımlanmıştır [71]. Standartlar yaşamın her alanında düzenlemeler sağlar. Sektörlerin içinde ve sektörler arası yapılan işlerde uygunluğun sağlanması için birer yol gösterici görevindedirler. Standartların planlanması, oluşturulması, yayımlanması ve düzenlenmesi gibi hususlar standardizasyon olarak ifade edilebilmektedir. Standardizasyon görevini ise ulusal ve uluslararası, kurumsal olan veya kurumsal olmayan çeşitli kuruluşlar üstlenmektedir. Bu kuruluşlardan en bilindikleri; ISO ve IEC kuruluşlarıdır.

ISO yani Uluslararası Standardizasyon Kuruluşu, her ülkeden bir üyelik olmak üzere 170 standart kuruluşunun üyeliğine sahip bağımsız bir kuruluştur. 1946 yılında, 25 ülkeden 65 temsilcinin Londra'da buluşmasıyla temelleri atılan ISO, 1947 yılında kurulmuştur. Genel merkezi İsviçre'nin Cenevre şehrinde bulunmaktadır [72].

ISO tarafınca herhangi bir sektördeki pazar ihtiyacına karşılamak adına bir standardın oluşturulması ve yayımlanması için ciddi bir süreç yürütülmektedir. Birbirinden farklı görevler üstlenen ve farklı bakış açılarının standardın oluşturulmasına dahil eden teknik komiteler bu sürecin en önemli organlarındandır. Bu çalışmanın hazırlandığı tarih itibari ile ISO bünyesinde bulunan, standartlarla ilgili geliştirici faaliyetlerle ilgilenen çeşitli uzmanlıklardan 828 adet teknik komite ve bunun doğrultusunda ISO Standartları kataloğunda yer alan 25204'ten fazla standart mevcuttur. [72]

ISO bünyesinde bulunan 3 çeşit üyelik mevcuttur. Bu üyelikler *'full'*, '*correspondent*' ve '*subscriber*' olarak sıralanmaktadır. Full yani tam üyeliklerde standart ve politikaların geliştirilmesine katkı sağlamak, ISO çıktılarını satmak ve ISO yönetimine katılabilmek gibi yetkinlikler söz konusudur. Correspondent yani muhabir üyeler ise tam üyeler gibi standart ve politika geliştirmeye katılabilir ve ISO çıktılarını satabilirler. Ancak tam üyelikten farklı olarak ISO yönetiminde söz sahibi olamazlar. Son olarak subscriber yani abone üyelik ise yalnızca standartların geliştirilmesinde rol oynayabilmektedirler. Politika geliştirmek, standartların satışını gerçekleştirmek ya da ISO yönetimine katılmak abone üyeler için söz konusu değildir [73]. Türkiye, Türk Standartları Enstitüsü (TSE) üzerinden ISO'ya *Member Body* yani Üye Kuruluş olarak katkı sağlamaktadır. Ülkemiz tarafından 3 adet Politika Geliştirme Komitesi, 390 adet Teknik Komitede sorumluluk üstlenilmiştir [74].

ISO'nun eşgüdümlü olarak faaliyet gösterdiği çeşitli kuruluşların olduğu bilinmektedir. *International Electrotechnical Commission* (IEC) yani Uluslararası Elektroteknik Komisyonu ve *International Telecommunication Union (*ITU) yani Uluslararası Telekomünikasyon Birliği olarak bilinen bu uluslararası kuruluşlar ISO ile ortak çalışmalar yürütmektedirler [75].

IEC; 1906 yılında kurulmuştur ve ilk başkanı Lord Kelvin olarak bilinen, bilhassa elektrik ve ısı ile alakalı çalışmalarıyla nam salmış fizikçi William Thomson olmuştur. IEC; 'Elektroteknoloji' olarak adlandırılan elektrik, elektronik ve ilgili teknolojilerle alakalı standartları hazırlayarak yayımlayan uluslararası kuruluşların en önemlilerindendir [76]. Kuruluşun kendi ifadelerine göre IEC kurulduğu tarihten itibaren elektrik ve elektronik teknolojilerini daha verimli ve güvenilir hale getirilmesini sağlar [77].

170 ülkede 20000 uzman ile birlikte; bağımsız ve tarafsız bir standardizasyon platformu olan IEC'nin süreklilik esasına dayandırılarak geliştirilen güvenilir varlıkların elde edilmesini sağlayan teknik çerçeveyi oluşturduğu ifade edilebilmektedir. Bu kapsamda IEC yaklaşık 10.000 uluslararası standart yayımlamıştır. [78]

IEC yürüttüğü çalışmalar ile Birleşmiş Milletler Sürdürülebilir Kalkınma Amaçlarına destek vermektedir. Amaçların her biri için ciddi projeler ve yayınlar üreten IEC; iş süreçleri, hükümetler ve tüketicileri ortak paydada buluşturarak 17 amaç için ayrı ayrı yürütülen çalışmaların nihayetinde herkes için faydalı hale getirmeyi görev edinmiştir [79]. Sürdürülebilir Kalkınma Amaçları; Birleşmiş Milletler'in 193 üye ülkesi tarafından kararlaştırılan ve 2030 yılının sonuna dek gerçekleştirilmesi hedeflenen 17 amacı kapsar.

Bahsi geçen 17 amaç;

- "Yoksulluğa Son",
- "Açlığa Son",
- "Sağlık ve Kaliteli Yaşam",
- "Nitelikli Eğitim",
- "Toplumsal Cinsiyet Eşitliği",
- "Temiz Su ve Sanitasyon",
- "Erişilebilir ve Temiz Enerji",
- "İnsana Yakışır İş ve Ekonomik Büyüme",
- "Sanayi Yenilikçilik ve Altyapı",

- “Eşitsizliklerin Azaltılması”,
- “Sürdürülebilir Şehirler ve Topluluklar”,
- “Sorumlu Üretim ve Tüketim”,
- “İklim Eylemi”,
- “Sudaki Yaşam”,
- “Karasal Yaşam”,
- “Barış Adalet ve Güçlü Kurumlar”,
- “Amaçlar İçin Ortaklıklar”

olmak üzere sıralanmaktadır [80]. Birleşmiş Milletlerin kurucu üyelerinden olan Türkiye de bu amaçları desteklemektedir.

ISO’da olduğu gibi IEC bünyesinde de çeşitli alanlarda faaliyet gösteren teknik komiteler mevcuttur. Yıllar geçtikçe IEC bünyesinde bulunan teknik komitelerin kapsamı ve sayısı artış göstermiştir. Gelişen teknolojiye ayak uyduran IEC, teknik komitelerini yakıt hücresi teknolojilerinden giyilebilir elektronik cihazlara kadar geniş bir yelpazede çeşitlendirmiştir.

Bununla birlikte ulusal komiteler adı verilen temsilciliklerden de söz etmek gerekmektedir. IEC üyesi olan her ülkenin bir ulusal komitesi mevcuttur ve bu komitelerdeki temsilciler standardizasyon sürecinin uygunluk analizi çalışmalarında görev alırlar. IEC bünyesinde; 62 adet *full member* yani tam üye ve 28 adet *associate member* yani ortak üye olmak üzere toplamda 90 üyenin ulusal komitesi mevcuttur [81].

IEC için, yukarıda da söz edildiği üzere tam üye ve ortak üye olmak üzere iki tür üyelik söz konusudur. Tam üye olabilmek için, ülkenin ulusal komitesinin “IEC Statüleri ve Prosedür Kuralları”na uygunluğunun ispatlanıyor olması gerekmektedir. Tam üyeler teknik komitelerde görev alması için uzmanlarını gönderebilmekte, IEC yönetiminde söz sahibi olabilmektedir. Ortak üyeler ise belgelere erişim sağlayabilir ancak tam üye ülkelerde olduğu gibi diledikleri komitelere değil yalnızca sınırlı komitelere uzman gönderebilmektedirler. Bununla beraber tam üye ülkelerin aksine IEC yönetiminde söz sahibi olamamaktadırlar [81]. Türkiye IEC için tam üye ülke statüsündedir.

Ülkemizde ise, cumhuriyetin ilk yıllarından itibaren çeşitli standardizasyon faaliyetleri gerçekleştirilmiştir. 1934 yılında standardizasyon faaliyetleri için dönemin Ekonomi Bakanlığı’nın görevlendirilmesi ile kurumsal anlamda bir süreç başlatılmıştır [82].

Bahsi geçen ISO ve IEC standart kuruluşlarına, ülkemizi temsilen üye olan Türk Standartları Enstitüsü (TSE) Ekim 1954'te Türkiye Odalar ve Borsalar Birliği (TOBB) kapsamında hazırlanmış olan tüzük sonrasında kurulmuştur. Aralık 1959 tarihinde 'Bakanlar Kurulu Kararnamesi' olarak Resmî Gazetede yayımlanışının ardından, Kasım 1960'ta 132 Sayılı *Türk Standartları Enstitüsü Kuruluş Kanunu* ile TSE'nin kuruluş aşaması sonuçlandırmıştır.

TSE'nin ISO VE IEC'ye üyeliği ise ilk kuruluş tarihini takip eden yıllarda olmuştur. Üyelik tarihleri; ISO için 26 Mayıs 1955, IEC için ise 01 Ocak 1956 olarak kayıtlara geçmiştir.

Bilgi güvenliği yönetim sistemlerinin kurulumu ve yürütülmesi için yol gösterici olan, çeşitli standartlar bulunmaktadır. Bu standartlardan bazıları tüm sektörler için bilgi güvenliği yönetim sisteminin kurulumu ve yönetimi için tedbirler içerirken, bazıları yalnızca enerji sektörünü kapsamaktadır.

4.1. ISO/IEC 27001, ISO/IEC 27002 ve ISO/IEC 27019 Standartları

ISO/IEC 27000 ailesi bilgi güvenliğini sağlamak amacıyla geliştirilmiş standartlardan oluşmaktadır. Bünyesinde; "ISO/IEC 27001: Bilgi güvenliği, siber güvenlik ve kişisel gizliliğin korunması-Bilgi güvenliği yönetim sistemleri- Gereklilikler", "ISO/IEC 27002: Bilgi güvenliği kontrolleri", "ISO/IEC 27005: Bilgi güvenliği risk yönetimi" gibi standartları barındırmaktadır. Bilgi güvenliği kapsamında 60 standarttan fazlasının yer aldığı ISO/IEC 27000 ailesinde; sektöre özel standartlar yer almakta ve oldukça geniş perspektifte ilgili konulara değinilmektedir.

ISO/IEC 27001 standardı; bilgi güvenliği, siber güvenlik ve kişisel gizliliğin korunması konularını kapsayan bilgi güvenliği yönetim sistemlerinin gerekliliklerini açıklayan bir standarttır. Bilgi güvenliği yönetim sisteminin kurulması, yürütülmesi ve devamlı iyileştirmesi amacıyla yapılması gereken yükümlülükleri ifade etmektedir. Tüm kurum ve kuruluşlara uygun şekilde düzenlenmiş genel bir standarttır.

ISO/IEC 27001 standardı ana başlık ve bu ana başlıklar altında yer verilmiş alt başlıktan oluşmaktadır. Önsöz ve giriş yazılarının ardından, ilk üç bölümde kapsama, bağlayıcı atıflara ve terimler ile tanımlara yer verilmiştir. Daha sonra "Kuruluşun Bağlamı*"* bölümü gelmektedir ve bu bölüm; kuruluşlar ve kuruluşların bağlamı, ilgili tarafların gereksinimleri ve buna benzer hususları aydınlatabilmek için alt başlıklara ayrılmıştır. Kuruluş bağlamı

bölümünü ise "Liderlik*"* bölümü takip etmektedir, bu bölüm de yine kurumsal roller gibi konuların açıklanabilmesi adına alt başlıklara ayrılmıştır. Liderlik bölümü ve alt başlıklarında üst yönetimin sorumluluklarından söz edilmektedir. Bu bölümünün ardından ise alt başlıklarında risk analizi, risk değerlendirme, risk işleme gibi faaliyetleri düzenleyen ifadelerin yer aldığı "Planlama" bölümü gelmektedir. Planlama bölümünde risk yönetiminin planlanmasına ek olarak, bilgi güvenliği hedeflerine ulaşmak adına yapılacak planlama ve sistemde gerekli olan değişikliklerin planlanmasına yönelik yönergeler de bulunmaktadır. Bu bölümü ise; kaynaklar, yetkinlik, farkındalık, iletişim ve dokümante edilmiş bilgi kısımlarını içeren "Destek" bölümü takip etmektedir. Bir sonraki bölüm olan "İşletim" bölümünde; planlama bölümünde bahsi geçen eylemlerin uygulanması için yapılması gerekenleri planlayarak uygulamak ve kontrol etmek ile ilgili talimatlar, bilgi güvenliği risk değerlendirmeleri için yine planlama bölümünde bahsi geçen yönergeleri gerçekleştirilmesi ile ilgili talimatlar ve bilgi güvenliği risk işleme planının uygulanması ve sonuçlarının belgelenmiş şekilde saklanmasına yönelik talimatlar bulunmaktadır. Bu bölümü takip eden bölüm, üst yönetimin BGYS'ni düzenli aralıklarla kontrol etmesine dair hususlara alt başlıklarıyla birlikte yer verilmiş olan "Yönetimin Gözden Geçirmesi" bölümüdür. Son olarak "İyileştirme" bölümü ile birlikte sürekli iyileştirme ile uygunsuzluk ve düzeltici faaliyetler konularına değinilerek gerekli talimatlar açıklanmıştır.

Standart içerisinde; bahsi geçen on ana başlığı bilgi güvenliği yönetim sisteminde kapsam dışı bırakılamayacağı ifade edilmiştir.

Bu başlıklarla birlikte bilgi güvenliği kontrollerini içeren, özellikle denetimlerde kurum ve kuruluşların yükümlülüklerini ifade eden 'Ek A' bölümü bulunmaktadır. 'Ek A' kısmındaki yükümlülükler, standardın en son revizyonu olan 2022 versiyonunda düzenlenerek;

- 37 kontrolden oluşan "kurumsal kontroller",
- 8 kontrolden oluşan "kişi kontrolleri",
- 14 kontrolden oluşan "fiziksel kontroller",
- 34 kontrolden oluşan "teknolojik kontroller" altında toplanmıştır.

ISO/IEC 27001 standardının 2022 versiyonunda; bir önceki versiyonda 114 adet olan Ek-A kontrollerinin sayısı, bazı maddelerin bir başka madde ile birleştirtilmesiyle 93 kontrole düşmüştür. Bununla birlikte standardın 2022 versiyonunda 11 yeni kontrol maddesi bulunmaktadır.

Bu maddeler:

- “5.7- Tehdit istihbaratı”
- “5.23- Bulut hizmetlerinin kullanımı için bilgi güvenliği”
- “5.30- İş sürekliliği için bilgi ve iletişim teknolojisi hazırlığı”
- “7.4- Fiziksel güvenlik izleme”
- “8.9- Konfigürasyon (yapılandırma) yönetimi”
- “8.10- Bilgi silme”
- “8.11- Veri maskeleme”
- “8.12- Veri sızıntısını önleme”
- “8.16- İzleme faaliyetleri”
- “8.23- Web filtreleme”
- “8.28- Güvenli kodlama”

maddeleridir [83].

Aşağıdaki çizelgede ISO/IEC 27001 standardının Ek A maddelerinin; standardın bir önceki versiyonu olan 2017 versiyonu ve son versiyonu arasındaki farklılıklar özetlenmiştir [83].

Çizelge 4.1. ISO/IEC 27001:2013 ve ISO/IEC 27001:2022 versiyonlarının Ek A maddelerinin karşılaştırılması

ISO/IEC 27001:2022		**ISO/IEC 27001:2017**	
Madde No	**Kontrol**	**Madde No**	**Kontrol**
5.1	Bilgi güvenliği politikaları	A.5.1.1	Bilgi güvenliği için politikalar
		A.5.1.2	Bilgi güvenliği için politikaların gözden geçirilmesi
5.2	Bilgi güvenliği rolleri ve sorumlulukları	A.6.1.1	Bilgi güvenliği rolleri ve sorumlulukları
5.3	Görevlerin ayrılığı	A.6.1.2	Görevlerin ayrılığı
5.4	Yönetim sorumlulukları	A.7.2.1	Yönetimin Sorumlulukları
5.5	Yetkililerle iletişim	A.6.1.3	Otoritelerle İletişim
5.6	Özel ilgi gruplarıyla iletişim	A.6.1.4	Özel ilgi gruplarıyla iletişim
5.7	Tehdit istihbaratı	-	*2022 versiyonunda eklenen bir maddedir, eski versiyonda karşılığı bulunmamaktadır.*
5.8	Proje yönetiminde bilgi güvenliği	A.6.1.5	Proje yönetiminde bilgi güvenliği
		A.14.1.1	Bilgi güvenliği gereksinimleri analiz ve belirtimi

ISO/IEC 27001:2022		ISO/IEC 27001:2017	
Madde No	**Kontrol**	**Madde No**	**Kontrol**
5.9	Bilgi envanteri ve diğer ilgili varlıklar	A.8.1.1	Varlıkların envanteri
		A.8.1.2	Varlıkları sahipliği
5.10	Bilgilerin ve diğer ilişkili varlıkların kabul edilebilir kullanımı	A.8.1.3	Varlıkların kabul edilebilir kullanımı
		A.8.2.3	Varlıkların kullanımı
5.11	Varlıkların iadesi	A.8.1.4	Varlıkların iadesi
5.12	Bilgilerin sınıflandırılması	A.8.2.1	Bilgi sınıflandırması
5.13	Bilgilerin etiketlenmesi	A.8.2.2	Bilgilerin etiketlenmesi
5.14	Bilgi transferi	A.13.2.1	Bilgi transfer politikaları ve prosedürleri
		A.13.2.2	Bilgi transferindeki anlaşmalar
		A.13.2.3	Elektronik mesajlaşma
5.15	Erişim kontrolü	A.9.1.1	Erişim kontrol politikası
		A.9.1.2	Ağlara ve ağ hizmetlerine erişim
5.16	Kimlik yönetimi	A.9.2.1	Kullanıcı kaydetme ve kayıt silme
5.17	Kimlik doğrulama bilgileri	A.9.2.4	Kullanıcılara ait gizli kimlik doğrulama bilgilerinin yönetimi
		A.9.3.1	Gizli kimlik doğrulama bilgisinin kullanımı
		A.9.4.3	Parola yönetim sistemi
5.18	Erişim hakları	A.9.2.2	Kullanıcı erişimine izin verme
		A.9.2.5	Kullanıcı erişim haklarının gözden geçirilmesi
		A.9.2.6	Erişim haklarının kaldırılması veya düzenlenmesi
5.19	Tedarikçi ilişkilerinde bilgi güvenliği	A.15.1.1	Tedarikçi ilişkileri için bilgi güvenliği politikası
5.20	Tedarikçi anlaşmalarında bilgi güvenliğinin ele alınması	A.15.1.2	Tedarikçi anlaşmalarında güvenliği ifade etme
5.21	Bilgi ve iletişim teknolojisi (BİT) tedarik zincirinde bilgi güvenliğini yönetme	A.15.1.3	Bilgi ve iletişim teknolojileri tedarik zinciri
5.22	Tedarikçi hizmetlerinin izlenmesi, gözden geçirilmesi ve değişiklik yönetimi	A.15.2.1	Tedarikçi hizmetlerini izleme ve gözden geçirme
		A.15.2.2	Tedarikçi hizmetlerindeki değişiklikleri yönetme
5.23	Bulut hizmetlerinin kullanımı için bilgi güvenliği	-	*2022 versiyonunda eklenen bir maddedir, eski versiyonda karşılığı bulunmamaktadır.*
5.24	Bilgi güvenliği ihlal olayı yönetimi planlaması ve hazırlığı	A.16.1.1	Sorumluluklar ve prosedürler

ISO/IEC 27001:2022		ISO/IEC 27001:2017	
Madde No	**Kontrol**	**Madde No**	**Kontrol**
5.25	Bilgi güvenliği ihlal olaylarını değerlendirme ve karar verme	A.16.1.4	Bilgi güvenliği olaylarında değerlendirme ve karar verme
5.26	Bilgi güvenliği ihlal olaylarına yanıt verme	A.16.1.5	Bilgi güvenliği ihlal olaylarına yanıt verme
5.27	Bilgi güvenliği ihlal olaylarından ders çıkarma	A.16.1.6	Bilgi güvenliği ihlal olaylarından ders çıkarma
5.28	Kanıt toplama	A.16.1.7	Kanıt toplama
5.29	Kesinti sırasında bilgi güvenliği	A.17.1.1	Bilgi güvenliği sürekliliğinin planlanması
		A.17.1.2	Bilgi güvenliği sürekliliğinin uygulanması
		A.17.1.3	Bilgi güvenliği sürekliliğinin doğrulanması, gözden geçirilmesi ve değerlendirilmesi
5.30	İş sürekliliği için BİT hazırlığı	-	*2022 versiyonunda eklenen bir maddedir, eski versiyonda karşılığı bulunmamaktadır.*
5.31	Yasal, meşru, düzenleyici ve sözleşmeye tabi gereklilikler	A.18.1.1	Yasal, meşru, düzenleyici ve sözleşmeye tabi gereklilikler
		A.18.1.5	Kriptografik kontrollerin düzenlenmesi
5.32	Fikri mülkiyet hakları	A.18.1.2	Fikri mülkiyet hakları
5.33	Kayıtların korunması	A.18.1.3	Kayıtların korunması
5.34	Kişiyi tespit bilgisinin (PII) gizliliği ve korunması	A.18.1.4	Kişi tespit bilgisinin gizliliği ve korunması
5.35	Bilgi güvenliğinin bağımsız gözden geçirilmesi	A.18.2.1	Bilgi güvenliğinin bağımsız gözden geçirmesi
5.36	Bilgi güvenliğine yönelik politikalar, kurallar ve standartlara uygunluk	A.18.2.2	Güvenlik politikaları ve standartları ile uyum
		A.18.2.3	Teknik uyum gözden geçirmesi
5.37	Dokümante edilmiş işletim prosedürleri	A.12.1.1	Yazılı işletim prosedürleri
6.1	Tarama	A.7.1.1	Tarama
6.2	İstihdam hüküm ve koşulları	A.7.1.2	İstihdam hüküm ve koşulları
6.3	Bilgi güvenliği farkındalığı, eğitim ve öğretim	A.7.2.2	Bilgi güvenliği farkındalığı, eğitim ve öğretimi
6.4	Disiplin prosesi	A.7.2.3	Disiplin süreci
6.5	İstihdamın sona ermesinden veya değiştirilmesinden sonraki sorumluluklar	A.7.3.1	İstihdam sorumluluklarının sonlandırılması veya değiştirilmesi
6.6	Gizlilik veya ifşa etmeme anlaşmaları	A.13.2.4	Gizlilik ya da ifşa etmeme anlaşmaları
6.7	Uzaktan çalışma	A.6.2.2	Uzaktan çalışma
6.8	Bilgi güvenliği olayı raporlanması	A.16.1.2	Bilgi güvenliği olaylarının raporlanması

ISO/IEC 27001:2022		ISO/IEC 27001:2017	
Madde No	**Kontrol**	**Madde No**	**Kontrol**
		A.16.1.3	Bilgi güvenliği açıklarının raporlanması
7.1	Fiziksel güvenlik sınırları	A.11.1.1	Fiziksel güvenlik sınırı
7.2	Fiziksel giriş	A.11.1.2	Fiziksel giriş kontrolleri
		A.11.1.6	Teslimat ve yükleme alanları
7.3	Ofislerin, odaların ve tesislerin güvenliğini sağlama	A.11.1.3	Ofislerin, odaların ve tesislerin güvenliğinin sağlanması
7.4	Fiziksel güvenlik izleme	-	*2022 versiyonunda eklenen bir maddedir, eski versiyonda karşılığı bulunmamaktadır.*
7.5	Fiziksel ve çevresel tehditlere karşı koruma	A.11.1.4	Dış ve çevresel tehditlere karşı koruma
7.6	Güvenli alanlarda çalışma	A.11.1.5	Güvenli alanlarda çalışma
7.7	Temiz masa ve temiz ekran	A.11.2.9	Temiz masa temiz ekran politikası
7.8	Ekipman konumlandırma ve koruma	A.11.2.1	Teçhizat yerleştirme ve koruma
		A.11.2.8	Gözetimsiz kullanıcı teçhizatı
7.9	Kuruluş dışındaki varlıkların güvenliği	A.11.2.6	Kuruluş dışındaki teçhizat ve varlıkların güvenliği
7.10	Depolama ortamı	A.8.3.1	Taşınabilir ortam yönetimi
		A.8.3.2	Ortamın yok edilmesi
		A.8.3.3	Fiziksel ortam aktarımı
		A.11.2.5	Varlıkların taşınması
7.11	Destekleyici altyapı hizmetleri	A.11.2.2	Destekleyici altyapı hizmetleri
7.12	Kablo güvenliği	A.11.2.3	Kablo güvenliği
7.13	Ekipman bakımı	A.11.2.4	Teçhizat bakımı
7.14	Ekipmanın güvenli bir şekilde yok edilmesi veya tekrar kullanılması	A.11.2.7	Teçhizatın güvenli yok edilmesi ve tekrar kullanılması
8.1	Kullanıcı uç nokta cihazları	A.6.2.1	Mobil cihaz politikası
8.2	Ayrıcalıklı erişim hakları	A.9.2.3	Ayrıcalıklı erişim haklarının yönetimi
8.3	Bilgi erişim kısıtlaması	A.9.4.1	Bilgiye erişimin kısıtlanması
8.4	Kaynak koduna erişim	A.9.4.5	Program kaynak koduna erişim kontrolü
8.5	Güvenli kimlik doğrulama	A.9.4.2	Güvenli oturum açma prosedürleri
8.6	Kapasite yönetimi	A.12.1.3	Kapasite yönetimi

ISO/IEC 27001:2022		ISO/IEC 27001:2017	
Madde No	**Kontrol**	**Madde No**	**Kontrol**
8.7	Kötü amaçlı yazılıma karşı koruma	A.12.2.1	Kötücül yazılımlara karşı kontroller
8.8	Teknik açıklıkların yönetimi	A.12.6.1	Teknik açıklıkların yönetimi
8.9	Konfigürasyon (yapılandırma) yönetimi	-	*2022 versiyonunda eklenen bir maddedir, eski versiyonda karşılığı bulunmamaktadır.*
8.10	Bilgi silme	-	*2022 versiyonunda eklenen bir maddedir, eski versiyonda karşılığı bulunmamaktadır.*
8.11	Veri maskeleme	-	*2022 versiyonunda eklenen bir maddedir, eski versiyonda karşılığı bulunmamaktadır.*
8.12	Veri sızıntısını önleme	-	*2022 versiyonunda eklenen bir maddedir, eski versiyonda karşılığı bulunmamaktadır.*
8.13	Bilgi yedekleme	A.12.3.1	Bilgi yedekleme
8.14	Bilgi işleme tesislerinin yedek fazlalığı	A.17.2.1	Bilgi işleme olanaklarının erişilebilirliği
8.15	Kaydetme (log tutma)	A.12.4.1	Olay kaydetme
		A.12.4.2	Kayıt bilgisinin korunması
		A.12.4.3	Yönetici ve operatör kayıtları
8.16	İzleme faaliyetleri	-	*2022 versiyonunda eklenen bir maddedir, eski versiyonda karşılığı bulunmamaktadır.*
8.17	Saat senkronizasyonu	A.12.4.4	Saat senkronizasyonu
8.18	Ayrıcalıklı destek programlarının kullanımı	A.9.4.4	Ayrıcalıklı destek programlarının kullanımı
8.19	İşletim sistemlerine yazılım kurulumu	A.12.5.1	İşletimsel sistemler üzerine yazılım kurulumu
		A.12.6.2	Yazılım kurulumu kısıtlamaları
8.20	Ağ güvenliği	A.13.1.1	Ağ kontrolleri
8.21	Ağ hizmetlerinin güvenliği	A.13.1.2	Ağ hizmetlerinin güvenliği
8.22	Ağların ayrımı	A.13.1.3	Ağlarda ayrım
8.23	Web filtreleme	-	*2022 versiyonunda eklenen bir maddedir, eski versiyonda karşılığı bulunmamaktadır.*
8.24	Kriptografi (şifreleme) kullanımı	A.10.1.1	Kriptografik kontrollerin kullanımına ilişkin politika
		A.10.1.2	Anahtar yönetimi
8.25	Güvenli geliştirme yaşam döngüsü	A.14.2.1	Güvenli geliştirme politikası

ISO/IEC 27001:2022		ISO/IEC 27001:2017	
Madde No	**Kontrol**	**Madde No**	**Kontrol**
8.26	Uygulama güvenlik gereklilikleri	A.14.1.2	Halka açık ağlardaki uygulama hizmetlerinin güvenliğinin sağlanması
		A.14.1.3	Uygulama hizmet işlemlerinin korunması
8.27	Güvenli sistem mimarisi ve mühendislik ilkeleri	A.14.2.5	Güvenli sistem mühendisliği prensipleri
8.28	Güvenli kodlama	-	*2022 versiyonunda eklenen bir maddedir, eski versiyonda karşılığı bulunmamaktadır.*
8.29	Geliştirme ve kabul aşamasında güvenlik testleri	A.14.2.8	Sistem güvenlik testi
		A.14.2.9	Sistem kabul testi
8.30	Dış kaynak yoluyla geliştirme	A.14.2.7	Dışarıdan sağlanan geliştirme
8.31	Geliştirme, test ve canlı (gerçek) ortamlarının ayrılması	A.12.1.4	Geliştirme, test ve işletim ortamlarının birbirinden ayrılması
		A.14.2.6	Güvenli geliştirme ortamı
8.32	Değişiklik yönetimi	A.12.1.2	Değişiklik yönetimi
		A.14.2.2	Sistem değişiklik kontrolü prosedürleri
		A.14.2.3	İşletim platformu değişikliklerden sonra uygulamaların teknik gözden geçirmesi
		A.14.2.4	Yazılım paketlerindeki değişikliklerdeki kısıtlamalar
8.33	Test bilgisi	A.14.3.1	Test verisinin korunması
8.34	Tetkik testi sırasında bilgi sistemlerinin korunması	A.12.7.1	Bilgi sistemlerinin tetkik kontrolleri

ISO/IEC 27002 standardı; ISO/IEC 27001 standardının uygulama prensiplerini içeren, kontrol maddelerini açıklayarak referans niteliği taşıyan bir kılavuz standardıdır. ISO/IEC 27002 standardı içerisinde, her bir bölümün standartta yer almasının amacı açıklandıktan sonra kontrol ve uygulama kılavuzu ve bunları takip eden diğer bilgiler bölümlerinde ilgili açıklamalara yer verilmiştir. ISO/IEC 27001 standardının 2022 yılında yeni versiyonunu yayınlaması ile birlikte ISO/IEC 27002 standardı da yenilenmiştir.

ISO/IEC 27002 standardının 2022 versiyonunda; ISO/IEC 27001 standardının “Ek A” olarak isimlendirilen kısmında yer alan kontrollerin her biri için detaylı açıklamalar bulunmaktadır. Her kontrol maddesi için künye olarak tabir edilebilecek bir nitelikler

tablosuna yer verilmiştir. Bu tablo içerisinde kontrol maddesinin; tipi yani önleyici mi tespit edici mi yoksa düzeltici mi olduğu bilgisi, bilgi güvenliğinin temel unsurlarından hangisiyle ilişkisi olduğu, siber güvenlik konseptlerinden hangisine dahil olduğu, operasyonel yetenekleri ve hangi güvenlik alanı içinde bulunduğuna dair bilgiler bulunmaktadır. Bu tablonun altında yine bir önceki versiyondaki gibi kontrol maddesinin amacı, uygulama kılavuzu ve diğer bilgiler kısımlarında kontrol maddelerinin tamamı için bilgilendirici açıklamalar bulunmaktadır.

Kurumlarda ISO/IEC 27001 standardının gerektirdiği yükümlülükler uygulanmaktadır. Özellikle ilk on madde içerisinde yer alan, düzenli aralıklarla planlanarak gerçekleştirilmesi gereken İç Tetkik ve Yönetimin Gözden Geçirmesi (YGG) faaliyetlerinin yapılması ve belgelendirilmesi gerekmektedir. İç tetkiklerin belirlenen kriterlere uygun şekilde gerçekleştirilmesinin ardından YGG toplantısı düzenlenmektedir. Üst yönetimin katılımı ile gerçekleştirilen toplantıda; bir önceki toplantıda alınan kararların mevcut durumundan, en az yıllık periyotlarda güncellenmesi gereken risk değerlendirmesinden, iç tetkik sonuçlarından, düzeltici ve iyileştirici faaliyetler ile var ise uygunsuzluklardan, sürekli iyileştirme kapsamında gerçekleştirilen farkındalık eğitimleri gibi hususlardan söz edilmektedir.

ISO/IEC 27019 standardı ise ISO/IEC 27001 ailesi bünyesinde enerji sektöründe kullanılmak üzere yayımlanmıştır. İçerisinde sektör özelindeki endüstriyel kontrol sistemlerinin güvenliğine yönelik kontroller bulunmaktadır.

Tam olarak ismi “ISO/IEC 27019 Enerji Hizmet Endüstrisi İçin Bilgi Güvenliği Kontrolleri” olan standarda, ISO’nun web sitesinin yanı sıra diğer ISO/IEC 27000 ailesi bünyesindeki standartlarında olduğu gibi TSE üzerinden erişim sağlanabilmektedir.

ISO/IEC 27019 standardı 18 ana bölümden oluşmaktadır. Bu 18 bölüm, standart yayınladığında yürürlükte olan ISO/IEC 27001 “Ek A” kontrollerine ve dolayısıyla ISO/IEC 27002 standartlarına dayanmaktadır. Standartta “Ek A” kontrolleri enerji sektörüne uygun bir bakış açısıyla değerlendirilerek dokümante edilmiştir. Ayrıca standardın “Ek A” bölümde enerji sektörüne özel kontroller özetlenmiştir. ISO/IEC 27019’un “Ek A” bölümünde ilgili bölümün ISO/IEC 27001 standardının “Ek A” bölümüne ilave olduğu ibaresi yer almaktadır.

ISO/IEC 27019 standardı ile ilgili en önemli husus standardın bir kılavuz görevi görmesidir. Tek başına bir bilgi güvenliği sisteminin kurulması ve yönetilmesi için uygun bir standart değildir. Ancak enerji sektöründe, ISO/IEC 27001 ve ISO/IEC 27002 standartlarına dayanarak kurulmuş bir sistem için ek güvenlik prensiplerinin değerlendirilmesi amacıyla yol gösterici olmaktadır.

4.2. NIST 800-53 ve NIST 800-82

National Institute of Satndards and Technology (NIST) yani "Ulusal Standartlar ve Teknoloji Enstitiüsü"; ABD Ticaret Bakanlığı'na bağlı 1901 yılında faaliyete geçen bir kuruluştur. Enerji, siber güvenlik, adli bilişim ve daha birçok alanda çok çeşitli konu ve ürünler için ölçüm ve standartların yanı sıra çeşitli teknolojik hizmetler de geliştirmektedir.

Geliştirmiş olduğu standartlardan biri de ABD Federal Hükümetinin bilgi güvenliği ve bilgi güvenliği yönetim sistemleri hususlarındaki ihtiyaçlarının karşılanması için yürürlüğe giren *NIST Special Publication 800* (NIST SP 800) serisidir. NIST SP 800 standartlar serisi; ISO/IEC 27000 ailesi ile benzer nitelikler taşımaktadır.

NIST SP 800-53 kodlu doküman *Security and Privacy Controls for Information System and Organizations* ismini taşımaktadır. Türkçeye "Bilgi Sistemleri ve Organizasyonları için Güvenlik ve Gizlilik Kontrolleri" olarak çevrilebilen dokümanın 2020 yılının Eylül ayı itibariyle 5.revizyonu yayımlanmış ve güncel olarak yürürlükte bulunmaktadır. NIST SP 800-53 kontrollerinin ISO/IEC 27001 ve onun kılavuzu niteliği taşıyan ISO/IEC 27002 standartlarına karşılık geldiği söylenebilmektedir.

Dokümanın hazırlanmasındaki amacın birey, ülke ve kurumların saldırı, hata ya da doğal afetler benzeri durumlardan meydana gelen problemlere karşı güvenlik ve gizliliğin korunmasını sağlamak olduğu belirtilmiştir.

NIST SP 800-53 dokümanı 3 ana bölümden oluşmaktadır. Birinci bölümde bu dokümanın amacı, kime ve neye hizmet ettiği gibi konuların açıklandığı bir giriş kısmı yer almaktadır. İkinci bölüm, kontrollerin genel mantığının açıklandığı temel esaslar bölümünden oluşmaktadır. Üçüncü bölüm ise kontrollerin yer aldığı bölümdür. Bu bölümde çeşitli konu başlıklarına atanmış kontroller ve uygulama esasları bulunmaktadır. Kontroller bölümü ISO/IEC 27001'in Ek A kontrollerini açıklayan ISO/IEC 27002 standardına benzer şekilde düzenlenmiştir. Standardın yer aldığı web sitesinde NIST SP 800-53 kontrolleri ile ISO/IEC

27001 kontrollerinin karşılaştırıldığı çeşitli dokümanlar mevcuttur. Bu dokümanlar kapsamında kontrollerin büyük ölçüde birbiri ile örtüştüğü görülmektedir.

Standardın yer aldığı web sitesinin ilgili sayfasında NIST SP 800-53 kontrollerinin 53 "*cyber securtiy framework*" yani siber güvenlik çerçevesi adı verilen sistem ile eşleştirmelerinin bulunduğu bir doküman yer almaktadır. Bu dokümana göre NIST SP 800-53; CSF sistemine uygun olarak kontrollerini 5 kategori profili altında toplamıştır. Bu kategoriler; "*Identify*", "*Protect*", "*Detect*", "*Respond*" ve "*Recover*" olmak üzere sıralanmaktadır.

"Identify" yani "Tanımla" kategorisinde; varlık yönetimi, risk yönetimi, tedarik zinciri yönetimi gibi konu başlıkları ve bu hususlardaki tanımlamaya yönelik kontroller bulunmaktadır. "*Protect*" yani "Koru" kısmında; farkındalığa, erişim kontrolüne, veri güvenliğine, bilgi güvenliği süreçlerine yönelik çeşitli kontroller yer almaktadır.

"*Detect*" yani "Tespit Et"; anomali ve olayların tespiti, bilişim sistemlerinin izlenmesi gibi konulara ait kontrolleri bünyesinde barındırmakta olan bir kategoridir.

"*Respond*" yani "Yanıtla" kategorisi; iç ve dış paydaşlarla iletişim, bilişim sistemlerinin ve süreçlerin analizi, analiz sonuçlarına göre tespit edilmiş yanıtların planlaması gibi kısımlara ait kontrolleri içermektedir.

Son olarak "*Recover*" yani "İyileştir"; iyileştirme ve geliştirme faaliyetlerinin planlanması ve yürütülmesi ile alakalı kontrollerin yer aldığı bir kategori olarak tanımlanmıştır.

NIST SP 800-53 içerisinde; kontrollerin esnek olduğundan ve tüm süreçle birlikte risk yönetiminin bir parçası olarak benimsenmesi gerektiğinden söz edilmiştir. Bu ifadeden kuruluşun yapısına göre kontrollerin özelleştirilebilir olduğu anlamı çıkmaktadır.

Bununla birlikte ISO/IEC 27000 ailesinde olduğu gibi NIST SP 800 serisinde de özelleştirilmiş rehberlerin varlığı bilinmektedir. Bunlardan bir tanesi NIST SP 800-82 kodlu "*Guide to Industrial Control Systems (ICS) Security*" olarak adlandırılmış Rehberdir.

NIST SP 800-82 Türkçeye "Operasyonel Teknolojilerin (OT) Güvenliği İçin Rehber" olarak çevrilebilmektedir ve güncel olarak 3.revizyonu olan Eylül 2023 tarihinde yayımlanmış versiyonu yürürlüktedir. Temel amacı OT sistemler için güvenlik protokollerine yönelik rehberlik etmektir. OT sistemler; endüstriyel kontrol sistemleri, ulaşım sistemleri, fiziksel erişim kontrol sistemleri, fiziksel ortam ölçüm ve izleme sistemleri gibi fiziksel ortamla

temas eden ya da fiziksel ortamlarla etkileşime giren cihazları yöneten programlanabilir sistemleri kapsamaktadır.

Doküman 6 ana bölümden oluşmaktadır. Başlangıç olarak "Giriş" bölümünde doküman hakkında genel bilgilendirmeler yer almaktadır. Ardından OT sistemlerden bahsedildiği bölüm gelmektedir. Bu bölümde SCADA, DCS, PLC gibi yapılar hakkında detaylı anlatımlar bulunmaktadır. Bununla birlikte OT sistemler ve IT (*Information Technology*) sistemlerin karşılaştırılmasına da yer verilmiştir.

Bahsi geçen karşılaştırmada çeşitli kategorilerde iki sistem arasında farklılıkların görünmesi ile birlikte; "Risk Yönetimi", "Kullanım Ömrü", "Bileşenlerin Konumu" gibi kategorilerdeki büyük farklar doğrudan göze çarpmaktadır. Örneğin risk yönetimi konusunda en büyük farklar; hata toleransının OT sistemlerde asla kabul edilememesi ve küçük kesintilerin dahi çok önemli olması ancak IT sistemlerde hata toleransının daha az önemli olması, OT sistemlerde en büyük risk etkisi can ya da ürün kaybı iken IT sistemlerde en büyük risk etkisinin iş operasyonlarındaki gecikme olması gibi hususlar belirtilmiştir. Kısaca bu kısımda; bir kuruluştaki siber güvenlik ve operasyonel stratejilerin karmaşıklığından ötürü süreçlerin hem IT uzmanları hem de OT uzmanlar tarafından iş birliği ile yürütülmesi gerektiğinin önemi vurgulanmaktadır.

Bu bölümün ardından; dokümanın "Ek C" kısmında tanımlanmış olan OT sistemler için tehdit kaynaklarına, zafiyetlere ve olaylara dayanarak risk ve açıklıkların azaltılması için OT siber güvenlik programının geliştirilmesini tartışan 3.bölüm gelmektedir. Sonraki bölüm olan 4.bölümde OT sistemlerinde, OT güvenliği için risk yönetiminin "Risk Yönetimi Çerçevesi" ne uygulanması açıklanırken 5.bölümde ağ segmentasyonu ve ağ bölümlendirmesi perspektifinden güvenliğin OT sistemlerde bulunan ağ mimarilerine entegrasyonu ile alakalı önerilere yer verilmiştir. Son olarak 6.bölümde NIST SP 800-53'tekine benzer şekilde "Siber Güvenlik Çerçevesi"nin OT sistemlere uygulanması için gerekli açıklamalar bulunmaktadır.

NIST SP 800-82'de "Ek" olarak yer alan 6 kısım daha vardır. Bunlardan ilk ikisi kısaltmalar ve terimlerden oluşmakta, üçüncüsü ise yukarıda da bahsedilmiş olan "Ek C" bölümüdür. OT güvenliği için araştırmaların ve organizasyonların derlendiği "EK D" bölümü ve OT güvenliği için araçlardan bahsedilen "Ek E" bölümlerinin ardından, NIST SP 800-53 kontrolleri ve OT sistemler için ek kontrollerin ilave edildiği "Ek F" bölümü yer almaktadır.

4.3. Cumhurbaşkanlığı Dijital Dönüşüm Ofisi Bilgi ve İletişim Güvenliği Rehberi

Cumhurbaşkanlığı Dijital Dönüşüm Ofisi; 30474 sayılı Resmî Gazete'de yayımlanan Kararname doğrultusunda 2018 yılında kurulmuştur. Kurulmasında; adından anlaşılabileceği üzere kamu kurum ve kuruluşlarının dijital dönüşümünü koordine etmek, başta siber güvenlik alanı olmak üzere yapay zekâ ve *big data* (büyük veri) alanlarında yapılacak çalışmaların tek bir yerden yürütülmesini sağlamak amacı güdülmüştür. Bu kapsamda 27 Temmuz 2020 tarihinde Dijital Dönüşüm Ofisi (DDO) tarafından, kamu kurumlarına ve kritik altyapı dahilindeki kuruluşlara yönelik bilgi güvenliği tedbirlerini içeren bir Rehber yayınlanmıştır [84]. 2019/2 sayılı Cumhurbaşkanlığı Bilgi ve İletişim Güvenliği Tedbirleri Genelgesi'nde belirtildiği üzere Rehber çalışmalarının yürütülmesi, Rehber'de belirtilen tedbirlerin uygulanması mecburidir. Rehber çalışmalarının yürütülmemesi, Rehber'in belirttiği kurallara uyulmaması veya Rehber denetiminin gerçekleştirilmemesi durumunda uygulanacak yaptırım belirlenmemiş, bu hususun ucu açık bırakılmıştır. Bununla birlikte Rehber'de belirtilene göre gerçekleştirilmeyen tedbirler için bulgu oluşturulup belirlenen sürede uygunsuzluğun giderilmesi beklenmektedir.

Rehberin içeriğinde çeşitli alanlara yönelik güvenliği sağlamak amacı ile hazırlanmış tedbir maddeleri ve bu tedbir maddelerinin denetim soruları yer almaktadır. Ayrıca Rehber'in uygulanmasındaki süreç içinde kullanılacak çeşitli form ve şablonlar da Rehber'in sonunda Ek olarak bulunmaktadır.

Rehber içerisinde "*Varlık Gruplarına Yönelik Güvenlik Tedbirleri*" başlığı altında; *'Ağ ve Sistemler', 'Uygulamalar', 'Taşınabilir Cihaz ve Ortamlar', 'IoT Cihazları', 'Personel' ve 'Fiziksel Mekanlar'* şeklinde sıralanmakta olan altı adet ana varlık grubu bulunmaktadır.

Bir diğer başlık olan *"Uygulama ve Teknoloji Alanlarına Yönelik Güvenlik Tedbirleri"* ise alt başlıklarında kişisel veri, anlık mesajlaşma, bulut bilişim, kripto uygulamaları ve kritik altyapı güvenliği ile birlikte yeni geliştirme ve tedarik hususlarında tedbirler içermektedir.

Son olarak "*Sıkılaştırma Tedbirleri*" başlığında; işletim sistemi, veri tabanı ve sunucu üzerine birtakım tedbirler toplanmıştır.

Rehber uyum sürecinde Kurumlar öncelikle varlık gruplarını belirlemektedir. Varlık grupları rehberde belirtilmiş olan ana varlık grupları ve alt varlık gruplarına göre belirlenir. Kurum envanterinde bulunan her bir varlık bir alt varlık grubu içerisinde tanımlanması gerekmektedir. Varlık grupları belirlendikten sonra; kritiklik derecelerinin belirlenmesi

amacı ile Rehber Eklerinde bulunan Anket çalışması yapılır. Hangi varlık grubuna hangi tedbirlerin uygulanması gerektiğine varlık grupları, kritiklik dereceleri ve Rehber'de belirlenmiş olan tedbir tanımlarına göre seçilir.

Rehber eklerinde bulunan "EK-C.3: Mevcut Durum ve Boşluk Analizi Formu" olarak isimlendirilen formun tedbirlerin uygulanma durumuna göre doldurulması gerekmektedir. Tedbirlerin varlık gruplarına uygulanma oranına göre doldurulan formda; tedbir tüm varlık gruplarına uygulanıyorsa "Tamamen", büyük çoğunluğuna uygulanıyorsa "Çoğunlukla", varlık gruplarının yalnızca bir bölümüne uygulanıyorsa "Kısmen", hiç uygulanmıyorsa "Hiç" ve eğer tedbirin uygulanması mümkün değilse "Uygulanamaz" ibareleri işlenmektedir.

Planlama bölümünün en son aşamasında, mevcut durum ve boşluk analizlerinin yapılmasının ardından kurumun eksiklerinin giderilmesi amacıyla bir planın belirlenmesi gerekmektedir. Bu gereklilik "EK C-4: Rehber Uygulama Yol Haritası Belirleme Formu" adıyla Rehberin eklerinde yer alan formun doldurulması ve takibi ile kayıt altına alınmaktadır. Bunun yanı sıra mevcut durum ve boşluk analizlerinin ardından telafi edici kontrollerin belirlenmesi ve kayıt altına alınması gerekmektedir. Rehber eklerinden bir diğeri olan "EK-C.5: Telafi Edici Kontrol Kayıt Formu" doldurularak tedbir maddesiyle aynı amacı taşıyan ve aynı sonuca ulaştırılabilen bir kontrolün, tedbir maddesinin yükümlülüklerini karşıladığı yazılı olarak ifade edilebilmektedir.

Kamu kurum ve kuruluşlarında, her yıl Bilgi ve İletişim Güvenliği Rehberi (BİGR) denetimleri gerçekleştirilmektedir. Rehber'de ISO Standartlarına benzer şekilde Enerji sektörüne özel tedbir tanımları da bulunmaktadır. Enerji sektöründeki kamu kurum ve kuruluşları; Rehber içerisinde bulunan ve tüm sektörleri kapsayan tedbirlerin yanı sıra bahsi geçen sektöre özel tedbirleri de uygulamak mecburiyetindedir [85]. Tedbir maddeleri ISO/IEC 27001 standardının maddeleri ile eşleştirilmiştir. Dolayısıyla Rehbere uyum süreci kolaylaşmaktadır. Enerji ve Tabii Kaynaklar Bakanlığı (ETKB) ile bağlı ve ilgili kuruluşlarının tamamında Rehber tedbirleri uygulanmakta ve bu kapsamda denetimler gerçekleştirilmektedir. Bağlı ve ilgili kuruluşların talep etmesi halinde BİGR denetimlerini ETKB personeli üstlenmiştir.

Bu kapsamda yine Dijital Dönüşüm Ofisi tarafından; 10 Ekim 2021 tarihinde "Bilgi ve İletişim Güvenliği Denetim Rehberi" yayımlanmıştır. Denetim Rehberi'nde; dokümanın amacının belirtildiği bölümde denetim metodolojisinin önemi vurgulanmıştır. Denetim

sürecinin bu talimatlara uygun olarak gerçekleştirilmesi mecburidir. Denetim Rehberi'nde yapılması gerekenler ve dokümantasyonu sağlanması gereken adımlar birbirini izleyen üç ana başlık altında toplanmıştır. Bu üç ana başlık; denetimin planlanmasını, sürecin gerçekleştirilmesini ve sonuçların değerlendirilerek raporlanmasını ifade etmektedir.

Öncelikle denetimin planlanması gerekmektedir. Bu aşamada işe denetim ekibinin belirlenmesiyle başlanmaktadır. Denetim ekibi; denetim koordinatörü ve en az iki denetçi olacak şekilde belirlenmeli ve ihtiyaç duyulması halinde teknik uzmanlar da denetim ekibine dahil edilmelidir. Kurum hakkında yeterince bilgi edindikten sonra denetim kapsamı kararlaştırılarak denetim kapsamına dahil edilecek varlık grupları belirlenmektedir. Ardından denetim programı hazırlanarak kuruma tebliğ edilmektedir.

Denetim esnasında sorulmak üzere; kurum için denetim kapsamına uygun olarak hazırlanmış, Denerim Rehberi'nde yer almakta olan kontrollerin ve ilgili soruların hazırlanması DDO tarafından teşvik edilmektedir. Ardından denetim sürecinin başlaması ve daha önce kuruma bildirilen denetim programına uygun şekilde sürdürülmesi gerekmektedir. Denetim prosedürlerinin Denetim Rehberi'nde bahsedilen denetim yöntemlerine uygun şekilde gerçekleştirilmesi beklenmektedir. Denetim Rehberi'ne göre denetimler; "Süreç Etkinliği" ve "Tedbir Etkinliği" şeklinde isimlendirilen hususları ölçmeyi hedeflemektedir. Bahsi geçen hususlar, Denetim Rehberi kapsamında "Ek" halinde yayımlanmıştır.

Denetçiler tarafından daha önce belirlenmiş olan varlık gruplarının ilgili tedbirleri denetlendikten sonra, yine Denetim Rehberi'nin ekinde yayınlanmış olan çalışma formlarının doldurulması beklenmektedir. Çalışma formlarında denetlenen tedbire dair kanıtların ve değerlendirmelerin yazılması beklenmektedir. Denetimin uygulama sürecinin etkinliğini değerlendiren "Süreç Etkinliği" tablosu ve tedbir maddelerinin etkinliğini ifade eden "Tedbir Etkinliği" tablosu ile birlikte Bulgu Tablosunun da hazırlanması gerekmektedir. Bulgu tablosu hazırlanırken; bulgunun kritiklik seviyesi ile izlenebilirliğini kolaylaştırmak adına denetim yılı ve denetim döneminin de yazılarak tabloda bulunması istenmiştir. Denetim sonuçlarının raporlanarak kuruma iletilmesiyle denetim süreci tamamlanmaktadır. Tüm bu aşamaların tamamlanmasının ve denetimin sonuçlandırılmasının ardından, denetimde elde edilen çıktıların ve sonuçların Dijital Dönüşüm Ofisi'ne gönderilmesi gerekmektedir.

5. LİTERATÜR ÖZETİ

Bu çalışmanın hazırlık aşamasında öncelikle literatür taraması gerçekleştirilmiştir. Anahtar kelimelerle yapılan aramalar sonucunda birçok farklı kaynağa göz gezdirilmiş, bu çalışma için faydalı olabilecek dokümanlar not edilerek çalışma için bir kütüphane oluşturulmuştur. Literatür araştırmaları için Türkçe ve İngilizce dillerinde taramalar yapılmıştır. Araştırmalar esnasında anahtar kelimeler seçilirken genelden özele yaklaşımı benimsenmiştir. İlk önce üzerinde çalışılması planlanan anket çalışmalarına benzer çalışmaların doğrudan enerji sektörüne ve/veya herhangi bir kamu kuruluşuna yönelik gerçekleştirilip gerçekleştirilmediği hususu üzerinde durulmuştur. Tez çalışmasının planı yapıldıktan ve içindekiler kısmı oluşturulduktan sonra bölüm başlıklarına uygun anahtar kelimeler taratılarak, bu konulara diğer çalışmalarda nasıl yer verildiği araştırılmıştır. Bununla birlikte tezin yazım aşamasında ihtiyaç olduğu takdirde yine literatüre başvurulmuştur.

Literatür taraması yapıldıktan sonra tarama esnasında alınan notlar tez çalışmasının yazılması sırasında kolaylık olması açısından bir çizelgeye aktarılmıştır. Çizelgedeki başlıklar; çalışmanın sahibi, çalışmanın tarihi, çalışmanın türü, çalışmanın başlığı, çalışmanın amacı, çalışmada kullanılan yöntem, çalışmada elde edilen sonuçlar ve ilgili çalışmadan hazırlanacak olan tez çalışmasında nasıl yararlanılabileceği ile alakalı notlar olmak üzere belirlenmiştir. Bu bölümde de çizelgede yer alan çalışmalardan bazıları ile ilgili açıklamalara yer verilmiştir.

Akay, 2014 yılında yayımlanan “Bilgi Güvenliği Yönetim Sistemleri: Bilgi Güvenliği Uygulama Mülakatları” isimli yüksek lisans tezini; BGYS ve ISO/IEC 27001 standardı hakkında bilgilendirmelerde bulunmak, bir BGYS sisteminin kuruluşu hakkında bilgi edinerek yol gösterici olma amacı güderek hazırlamıştır. Mülakat yöntemi kullanılan çalışmada, bilgi güvenliği süreçlerinin teorik ve pratik olarak aynı anda yürütülmesinin gerekliliği sonucuna varılmış, ISO/IEC 27001 belgesine sahip kuruluşların BGYS süreçleri değerlendirilip çözümlere ulaşılmıştır. Çalışmadan tezin Kavramsal Çerçeve ve BGYS İçin Yol Haritaları bölümleri yazılırken yararlanılmıştır.

Genco, 2020 yılında “Türkiye’de Kritik Altyapı ve Kritik Altyapıya Yönelik Tehditler” adlı makalesini yayınlamıştır. Yazar tarafın makalenin hazırlanmasındaki amaç, global çerçevede kritik altyapı kavramının tanımlanması ve ABD, AB ve ülkemizde kritik altyapılara yönelik tehditler ve alınması gereken tedbirleri ele almak olarak ifade edilmiştir. Çalışmanın sonunda kritik altyapıların, kurumların ve kritik altyapı sektöründe faaliyet

gösteren her türlü kuruluşun eşgüdümlü şekilde çalışması ile korunabileceğinden söz edilmiştir. Bununla beraber bu sektörlerde çalışmakta olan personelin ve kullanılan tüm cihazların yeterli olmasının önemi vurgulanmıştır. Çalışmadan tezin Kavramsal Çerçeve bölümünün Kritik Altyapılar alt başlığı hazırlanırken yararlanılmıştır.

Ottekin ve Çalık, "Enerji Sektöründe Bilgi Güvenliğinin Yönetilmesi: Mevzuat ve Standartlar" isimli çalışmalarını enerji sektöründe izlenmesi gereken BGYS süreçleri hakkında farkındalık oluşturmak amacı ile hazırlamışlardır. Sektörde ISO/IEC 27001, ISO/IEC 27011 ve ISO/IEC 27019 standartlarının dikkate alınması gerektiği sonucuna ulaşmışlardır. Ayrıca BGYS kurmak ve yürütmek için bir seneden fazla zaman geçmesi gerektiğini belirtmişlerdir. Çalışmadan tezin BGYS İçin Yol Haritaları bölümü yazılırken yararlanılmıştır.

Özbilen ve Çağlar tarafından hazırlanıp 2020 yılında yayınlanan "Türk Kamu Sektöründe Bilgi ve Bilişim Güvenliği" isimli makalenin amacı kamudaki bilgi güvenliği ve bilişim güvenliği hususlarının güncel olarak ne durumda olduğuna yönelik analizler yaparak çıktılar elde etmek ve değerlendirilen çıktılar doğrultusunda önerilere yer vermek olarak ifade edilmiştir. Yazarların çalışmadan elde ettikleri en önemli sonuç ülkemizin henüz bilgi toplumu olmadığı, fiziksel açıdan ve insan kaynağı bakımından yeterli donanıma sahip olamadığımız kanısıdır. Çalışmadan tezin Enerji Sektörü İçin BGYS'nin Önemi bölümünde yararlanılmıştır.

E. Şahinaslan, Ö. Şahinaslan ve Selimli tarafından hazırlanan "Siber Saldırıların Kritik Altyapılar Üzerindeki Etkileri" adlı bildiride; kritik altyapıları tehdit eden saldırıların, saldırıların sonucunun ve saldırılara alınabilecek tedbirlerin ortaya konulmasının amaçlandığı ifade edilmiştir. Çalışmanın sonuç kısmında kritik altyapılara karşı işlenen siber suçlar için ne gibi önlemler alınabileceği konusunda önerilerde bulunulmuştur. Kritik varlıkların ve varlıklar üzerindeki tehditlerin belirlenmesi, tehditlere karşı kontrollerin sağlanmasının önemli olduğu vurgulanmıştır. Çalışmadan tezin Kavramsal Çerçeve bölümünün Kritik Altyapılar alt başlığı ve Enerji Sektörü İçin BGYS'nin önemi bölümü hazırlanırken yararlanılmıştır.

Tez çalışmasında yürütülen anketler için yapılan literatür taraması sonucu yol gösterici olabileceği düşünülen dört kaynak belirlenmiştir. Belirlenen dört kaynak hazırlanırken kullanılan yöntem, bu tez çalışmasında olduğu gibi anket yöntemidir. Çalışmalardan özellikle anketin örneklemi için gruplar belirlenirken ve anketlerin soruları hazırlanırken

ilham alınmıştır. Bahsi geçen çalışmalar sırasıyla şu şekildedir; Tuygun tarafından hazırlanan “ISO/IEC 27001 Bilgi Güvenliği Yönetim Sistemi Standardının Kamu Kurumlarına Uygulanabilirliğinin Araştırılması: Ankara İli Örneği” isimli yüksek lisans tezi, Kılıç tarafından hazırlanan “ISO/IEC 27001 Bilgi Güvenliği Yönetim Sistemi Açısından Türkiye'de Hukuk Bürolarında Bilgi Güvenliği Yönetimi” isimli yüksek lisans tezi, Aslandağ tarafından hazırlanan “Bilgi Güvenliği Kavramı ve Bilgi Güvenliği Yönetim Sistemleri İle Şirket Performansı İlişkisine Dair Bir Uygulama” isimli yüksek lisans tezi ve son olarak Akdoğan tarafından hazırlanan “Kamu Kurumlarında Bilgi Güvenliği Yönetim Sistemleri İçin Politika Geliştirme Metodolojisi” isimli doktora tezi.

6. YÖNTEM

Bu bölümde enerji sektöründe bilgi güvenliği yönetim sistemlerinin, enerji sektöründe görev alan kişiler tarafından nasıl görüldüğü hususunda yürütülen çalışma açıklanmıştır.

6.1. Araştırmanın Amacı

Literatürde; enerji sektörü için bilgi güvenliği yönetim sistemlerinin etkilerini tespit etmek amacıyla hazırlanan çalışmalar hususunda eksiklikler olduğu görülmüştür. Bir önceki bölüm olan Literatür Özeti'nde de bahsedildiği üzere; uluslararası çalışmalarda kritik altyapılarda bilgi güvenliğinin sağlanmasına yönelik uygulanabilecek bilhassa teknolojik tedbirlere değinilmiş ve ülkemizdeki hukuk alanı gibi çeşitli alanlarda anket yönteminin benimsendiği çalışmalar gerçekleştirilmiştir. Ancak enerji sektörüne yönelik, bilgi güvenliğinin en zayıf halkası olan insanın bakış açısını temel alarak sistemin mevcut durumunun ölçüldüğü bir çalışmaya rastlanmamıştır. Oysaki ülkemizdeki kritik altyapılardan biri olan enerji sektöründe bilgi güvenliğinin sağlanması için kurulan sistemlerin mevcut durumunun ne olduğuna dair şeffaf bir çalışmanın ne kadar önemli olduğu tartışmaya açık dahi değildir. Bu çalışmada literatürdeki bahsi geçen eksiği gidermek amacı güdülmüştür. Bu sebeple bu çalışmada kullanılmak üzere, çeşitli gruplara yönelik anketler hazırlanmıştır. Anketlerde yer alan sorular ISO/IEC 27001 standardı baz alınarak belirlenmiştir.

Anketlerden ilki enerji sektöründe görev alan kişilere yönelik hazırlanan Personel anketidir. Personel anketi için düzenlenen sorular aşağıdaki çizelgede bulunmaktadır.

Çizelge 6.1.1. Personel için hazırlanan anketin soruları

1	Kurumda, bilgi güvenliği yönetim sistemi iyi şekilde yürütülmektedir.
2	Bilgi güvenliği yönetim sistemi standardı kapsamında farkındalık eğitimleri alınmaktadır.
3	Bilgi güvenliği yönetim sistemi ile ilgili verilen eğitimler yeterlidir.
4	Bilgi güvenliği yönetim sistemi kapsamında yapılan faaliyetler sayesinde iş süreçleri hızlı ve sağlıklı şekilde yönetilmektedir.
5	Kurum ve iş yapılan kuruluşların bilgi güvenliği yönetim sistemi sertifikasının olması, bilgi güvenliğini sağlamaktadır.
6	Bilgi güvenliği yönetim sistemi standardı, bilgi güvenliği konusundaki ihlalleri engellemektedir.
7	Bilgi güvenliği yönetim sistemi kapsamında yapılan faaliyetler, kurumsal risk analizinin gerçekleştirilmesine katkı sağlamaktadır.
8	Bilgi güvenliği yönetim sisteminin kalitesini ölçmek adına anketler yapılmaktadır.
9	Bilgi güvenliği politikası kapsamında meydana gelen değişimler, hali hazırdaki işleyişi etkilememektedir.

10	Bilgi güvenliği yönetim sistemi politikaları benimsenmekte ve desteklenmektedir.
11	BGYS birimi çalışanları, bilgi güvenliği yönetim sistemlerinin yürütülmesi sürecinde ekip dışında yer alan personelle iletişim halindedir.

Bu anketin çıktısından enerji sektöründe çalışan personelin, kuruluşun bilgi güvenliği yönetim sistemi kapsamında sahip olduğu ISO/IEC 27001 maddelerinden anket sorularıyla bağdaştırılanlarına bakış açısı görülmek istenmiştir. Böylece bilgi güvenliği yönetim sistemleri ile doğrudan ilişkili olmayan personelin BGYS hususundaki yaklaşımlarının değerlendirilmesi amaçlanmıştır. Sorular ile ISO/IEC 27001'in aşağıda yer verilen maddeleri ilişkilendirilmiştir.

- "5.2 Politika"
- "5.3 Kurumsal roller, sorumluluklar ve yetkiler"
- "7.2 Yetkinlik"
- "7.3 Farkındalık"
- "9.1 İzleme, ölçme, analiz ve değerlendirme"
- "10 İyileştirme"

Bir sonraki anket enerji sektöründe yer alan kuruluşların BGYS birimi çalışanları ve birimlerin BGYS sorumlularına yönelik düzenlenmiştir. Bu anketi çözenlerin hem BGYS'ye hem de kuruluşlarındaki sistemin işleyişine yönelik mevcut duruma dair fikirlerinin analiz edilebilmesi hedeflenmiştir. Hazırlanan sorular aşağıdaki çizelgede yer almaktadır.

Çizelge 6.1.2. BGYS çalışanlarına yönelik hazırlanan anketin soruları

1	Bilgi güvenliği yönetim sistemi birimi üyeleri, sistemin kurulumu ve yürütülmesi açısından sayıca yeterlidir.
2	Bilgi güvenliği yönetim sisteminin kurulması ve yürütülmesi için kurum personeli yeterli donanıma sahiptir.
3	Bilgi güvenliği yönetim sisteminin kurulması için danışmanlık hizmeti alınmıştır.
4	Bilgi güvenliği yönetim sisteminde süreçlerin düzgün yürütülebilmesi için BGYS Birimi personeli eğitim almıştır.
5	Bilgi güvenliği yönetim sistemi bütün kurum personeli ile iş birliği içerisinde yürütülmektedir.
6	Bilgi güvenliği yönetim sistemi politikaları herkes tarafından anlaşılır düzeyde hazırlanarak kurum personeliyle birlikte tüm iç ve dış paydaşlara bildirilmektedir.
7	Bilgi güvenliği yönetim sistemi politikaları kurum bünyesindeki bütün çalışanlar tarafından benimsenmektedir.
8	Bilgi güvenliği politikası kapsamında meydana gelen değişimler, çalışanlar tarafından hali hazırda işleyen sisteme tehdit olarak algılanmamaktadır.
9	Bilgi güvenliği standartlarına sahip olmak kurumsal bilgi güvenliğini sağlamaktadır.
10	Bilgi güvenliği standartları sayesinde, kurum içi ve kurum dışındaki kritik bilgi güvenliği gereksinimleri karşılanmaktadır.

11	Bilgi güvenliği sertifikasyonu sonrası süreçte, kurum personeli yeni kurallara uyum sağlamakta zorlanmamıştır.
12	BGYS Birimi, bilgi güvenliği yönetim sistemlerinin yürütülmesi sürecinde ekip dışında yer alan personelle iletişim halindedir.
13	Bilgi güvenliği yönetim sisteminin yürütülmesinde bütün birimler eşgüdümlü olarak dahil olmaktadır.
14	Bilgi güvenliği yönetim sistemi kapsamında, sürekli iyileştirmeler ve güncellemeler yapılmaktadır.
15	Bilgi güvenliği yönetim sisteminin kalitesini ölçmek adına yapılan faaliyetlerin çıktıları doğrultusunda gerekli aksiyonlar alınmaktadır.
16	Kurumda bilgi güvenliği standardı belgesine sahip olmadan önce bilgi güvenliği politikaları mevcut değildi.
17	Kurumda bilgi güvenliği standardı belgesi, belgeye sahip olmadan önceki bilgi güvenliği politikalarında bir değişikliğe sebep olmuştur.
18	Bilgi güvenliği yönetim sistemi kurulduktan sonra, öncesine göre güvenlik seviyesinde artış olmuştur.
19	Bilgi güvenliği yönetim sistemi kurulduktan sonra, öncesine göre kuruma yönelik siber saldırılarda azalma olmuştur.
20	Bilgi güvenliği yönetim sistemi kurulduktan sonra, öncesine göre kişisel ve kurumsal veri ihlallerinde azalma olmuştur.

Sorular ISO/IEC 27000'in aşağıdaki maddeleri baz alınarak hazırlanmıştır.

- "5.1 Liderlik ve bağlılık"
- "5.2 Politika"
- "5.3 Kurumsal roller, sorumluluklar ve yetkiler"
- "7.2 Yetkinlik"

Son anket ise enerji sektöründe yönetici görevi üstlenen çalışanlar için düzenlenmiş olan ankettir. BGYS için üst yönetimin rolü çok önemli olduğundan, yönetimde yer alan kimselerin sisteme olan bakış açısı çok önemlidir. Hazırlanan anket sorularının diğer iki ankette olduğu gibi yine ISO/IEC 27001 standardından maddelere uyumlu şekilde olması amaçlanmıştır. Böylece üst yönetimin bakış açısından BGYS'ye yönelik değerlendirmelerin analiz edilmesi hedeflenmektedir. Bu anket için hazırlanmış olan sorular aşağıda yer alan çizelgede bulunmaktadır.

Çizelge 6.1.3. Yönetim için hazırlanan anketin soruları

1	Bilgi güvenliği yönetim sistemi standartlarına sahip olmak bilgi güvenliğini korumaktadır.
2	Kritik bir güvenlik probleminde bilgi güvenliği yönetim sistemi koruma sağlamaktadır.
3	Bilgi güvenliği yönetim sistemi standartlarından uluslararası geçerliliği olan standartlara sahip olmak ulusal ve uluslararası çapta saygınlık sağlamaktadır.
4	Bilgi güvenliği yönetim sistemi standartlarının uygulanmasında yönetim önemli bir rol oynamaktadır.
5	Bilgi güvenliği yönetim sistemi politikaları kurum bünyesindeki bütün çalışanlar tarafından benimsenmektedir.

6	Bilgi güvenliği yönetimi süreçlerine, bütün birimler eşgüdümlü olarak dahil olmaktadır.
7	Bilgi güvenliği yönetimi kapsamında, sürekli iyileştirmeler ve güncellemeler yapılmaktadır.
8	Bilgi güvenliği yönetim sisteminin kalitesini ölçmek adına yapılan faaliyetlerin çıktıları doğrultusunda gerekli aksiyonlar alınmaktadır.
9	Üst yönetim bilgi güvenliği yönetim sistemini kontrol etmekte ve desteklemektedir.
10	Üst yönetimin bilgi güvenliği yönetim sistemine karşı yaklaşımı doğrultusunda sistem düzgün şekilde çalışmaktadır.
11	Üst yönetim bilgi güvenliği yönetim sistemi standardı uygulamalarından ayrıcalıklı tutulmamaktadır.

Yöneticiler için düzenlenen ankette genel hatlarıyla ISO/IEC 27001 standardının 5.bölümü olan "Liderlik" bölümü ve alt başlıkları referans alınmıştır. Bununla birlikte "9.1 İzleme, ölçme, analiz ve değerlendirme" bölümü de değerlendirmeye katılmıştır.

Anket soruları Bilgi Güvenliği Yöneti Sistemleri alanında uzman üç kişi tarafından incelenmiş ve teyit edilmiştir.

6.2. Evren ve Örneklem

Enerji sektöründeki BGYS ile alakalı mevcut durumun ölçülebilmesi amacıyla hazırlanan anketler için çalışmanın evreninin tüm enerji sektörüdür. Ancak sektördeki bütün çalışanlara ulaşmak mümkün değildir. Dolayısıyla her anket için belirli gruplar seçilerek anketlere katılım sağlamaları hususunda ricada bulunulmuştur. Online formatta hazırlanan anketler üst yönetimin izni ve desteği dahilinde e-posta yoluyla ilgili gruplara iletilmiştir. Üç anket için yürütülen veri toplama süreci toplamda 181 kişinin katılımıyla gerçekleştirilmiştir. Personel için hazırlanan anketi 57 kişi, BGYS sorumlularına yönelik anketi 77 kişi ve üst yönetim için hazırlanan anketi de 47 kişi doldurmuştur.

Personele yönelik hazırlanan anket ETKB Bilgi İşlem Dairesi Başkanlığı personeline gönderilmiştir. BGYS sorumluları anketi ise ETKB Merkez Teşkilat bünyesinde görev alan BGYS birimi personeline, ETKB Merkez Teşkilatında görev alan personellerden kendi birimlerinde BGYS sorumlusu olan personele ve ETKB bağlı kuruluşları ile ilgili kuruluşlarında BGYS biriminde görev alan çalışanlara iletilmiştir. Üst yönetim anketi de yine BGYS sorumluları anketindeki gibi ETKB Merkez Teşkilatı, ETKB bağlı kuruluşları ve ETKB ilgili kuruluşlarındaki daire başkanlığı ve üstü kademelerde görevli olan yöneticilerin katılımına sunulmuştur.

6.3. Verilerin Toplanması

Personele, BGYS birimi çalışanlarına ve yönetime uygun olarak hazırlanan anket soruları ilgili gruplara iletildikten sonra, elde edilen veriler daha önce belirlenen kriterlere göre analiz edilmiştir.

Bu aşamada anket sonucunda elde edilen verilerin yorumlanmasıyla ortaya çıkacak sonuçların doğru değerlendirilebilmesi açısından geçerlilik ve güvenilirlik testlerinin yapılmasının gerekli olduğu görülüp, testlerin gerçekleştirilebilmesi için SPSS programından yararlanılmıştır. Geçerlilik ve güvenilirlik testleri doğrultusunda değişkenlerin iç tutarlılıkları Cronbach Alpha analizi ile belirlenmiştir.

Likert tipi ölçeklerin kullanılması durumunda gerçekleştirilen güvenilirlik analizleri için çeşitli yöntemler kullanılabilmektedir. Literatür incelendiğinde benzer çalışmalarda sıklıkla Cronbach Alpha yöntemi kullanılmıştır. Bu çalışmanın analizinde gerçekleştirilen test olarak da yine bu yöntem tercih edilmiştir. Ancak ifade edildiği gibi başka yöntemlerin varlığı da bilinmektedir. Bahsi geçen diğer yöntemler şu şekilde sıralanabilir [86];

a) Split Half: Bu yöntem; soruların ikiye bölünerek her iki parça için de korelasyon katsayılarının hesaplanmasının ardından "Spearman Brown" formülü ile hesaplanmasına dayanmaktadır.

b) Guttman: Bu yöntem; varyans ve kovaryans değerlerine göre güvenirlik değerlerinin hesaplanması ile gerçekleştirilir.

c) Paralel ve Kesin Paralel: Bu yöntemler; varyans değerlerinin hesaplanmasının ardından sırasıyla paralel yöntemi için soruların varyanslarının eşit, kesin paralel yöntemi için ise soruların hem varyanslarının hem de ortalamalarının eşit olduğu varsayımına dayandırılarak gerçekleştirilen çeşitli işlemlere dayanmaktadır.

Cronbach Alpha analizi; Cronbach Alpha (α) katsayısının çeşitli yöntemlerle hesaplanmasının ardından aldığı değerin 1'e yakınlığına göre anketin güvenilirliği hakkında yorum yapma imkânı tanıyan bir analiz çeşididir. Bu çalışmada her bir anket için alpha değeri SPSS programında; ölçekte yer alan madde sayısının (k), toplam sütunun varyansının (σ_t^2) ve değişkenlerin her birinin varyansının (σ_i^2) hesaplanmasına dayanan bir formül kullanılarak bulunmuştur. Bahsi geçen formül; "$\alpha = \left[\frac{k}{k-1}\right]\left[1 - \left(\frac{\sigma_i^2}{\sigma_t^2}\right)\right]$" şeklindedir.

Hesaplamalar sonucunda; Personel anketi için α=0.91321, BGYS Çalışanları anketi için α=0.9658 ve Yönetim anketi için α=0.82185 olarak bulunmuştur.

Cronbach Alpha katsayısının değerine göre ölçeğin güvenilirliği şu şekilde kabul edilmektedir [87]:

- α >0 ve α ≤ 0,40 ise ölçek güvenilir değildir.
- α >0,40 ve α ≤ 0,60 ise ölçek düşük güvenilirliktedir.
- α >0,60 ve α ≤ 80 ise yeterince ise ölçek güvenilirdir.
- α >0,80 ve α ≤ 1,00 ise ölçek oldukça güvenilirdir

Buradan yola çıkarak üç anketin de oldukça güvenilir olduğu görülmektedir.

Aşağıdaki alt başlıklarda her anket için kapsam ve içeriğe dair detaylı açıklamalara yer verilmiştir.

6.3.1. Personel anketi

Enerji ve Tabii Kaynaklar Bakanlığı'nın Bilgi İşlem Dairesi Başkanlığı personeline yönelik hazırlanan 'Personel' anketine 57 kişi katılımda bulunmuştur. Anketin çevrimiçi bağlantısı katılımcılara Bilgi İşlem Dairesi Başkanlık makamı tarafından e-posta olarak iletilmiştir.

Anket içerisinde 14 adet soru bulunmaktadır. İlk 3 soru kişisel tanımlamaya yönelik sorulardır. Personelin kurum bünyesinde ne kadar süredir görev aldığı, şu an ETKB Bilgi İşlem Dairesi Başkanlığında hangi birimde görev aldığı ve bu görevde ne kadar süredir çalışmakta olduğu soruları sorulmuştur. Bilgi İşlem Dairesi Başkanlığında hangi birimde görev yapıldığının sorulduğu soruda cevaplar; Siber Güvenlik ve Bilişim Ağları Koordinatörlüğü, Bilişim Sistemleri Koordinatörlüğü, BT Destek Hizmetleri Müdürlüğü, Yazılım Koordinatörlüğü, Proje Yönetimi Koordinatörlüğü ve BT Personel ve Eğitim Müdürlüğü şeklinde belirlenmiştir. Geriye kalan sorularda 5 seçenekli likert tipi anket soruları sorulmuştur. Sorular için "Kesinlikle Katılmıyorum", "Katılmıyorum", "Kararsızım", "Katılıyorum" ve "Kesinlikle Katılıyorum" seçeneklerinden bir tanesinin işaretlenmesi istenmiştir. "Kesinlikle Katılıyorum" seçeneği için 5 puan, "Katılıyorum" seçeneği için 4 puan, "Kararsızım" seçeneği için 3 puan, "Katılmıyorum" seçeneği için 2 puan, "Kesinlikle Katılmıyorum" seçeneği için 1 puan olmak üzere değerlendirme yapılmıştır. Elde edilen yanıtlar hem genel olarak hem de personelin hangi birimde çalıştığına göre ayrı olmak üzere SPSS programında analiz edilmiştir.

6.3.2. BGYS birim çalışanları ve BGYS sorumluları anketi

Bu anket, ETKB BGYS biriminde görev alan personel, ETKB Merkez Teşkilattaki BGYS sorumluları ve ETKB bağlı ve ilgili kuruluşlarının BGYS birimlerinde görev alan kişilere yönelik hazırlanmış olup, ankete toplamda 77 kişi katılım sağlamıştır. Anketin çevrimiçi bağlantısı öncelikle Bakanlığın BGYS Birimine, ardından Bakanlık bünyesinde Merkez Teşkilatta görev alan BGYS sorumlularına üye oldukları e-posta grubu vasıtasıyla iletilmiştir. Ardından Bakanlığın bağlı ve ilgili kuruluşlarında BGYS birimlerinde görev almakta olan personele iletilmiş ve anketin dağıtımı tamamlanmıştır.

23 sorudan oluşan anketin ilk üç sorusu tanıma sorularıdır. Personel anketinde olduğu gibi, ilk soru katılımcının ne kadar süredir sektörde görev aldığı sorusudur. Bu sorunun ardından enerji sektöründe görev yaptığı kapsam öğrenilmek istenmiştir. Bu kapsamlar; elektrik, petrol, doğal gaz, maden, kömür, nükleer ve son olarak Enerji ve Tabii Kaynaklar Bakanlığının Merkez Teşkilatı olmak üzere kategorilere ayrılmıştır. Üçüncü soru ise katılımcının bu kapsamda ne kadar süredir çalıştığını ölçmek amacıyla sorulmuştur. Yine Personel anketinde olduğu gibi geriye kalan sorular, BGYS görevlilerinin bakış açısından sistemin mevcut durumunu analiz edebilmek amacıyla 5 seçenekli likert tipi sorulardan oluşacak şekilde hazırlanmıştır. Katılımcılardan "Kesinlikle Katılmıyorum", "Katılmıyorum", "Kararsızım", "Katılıyorum" ve "Kesinlikle Katılıyorum" seçeneklerinden kendilerine göre doğru olanını işaretlemeleri beklenmiştir. "Kesinlikle Katılıyorum" seçeneği için 5 puan, "Katılıyorum" seçeneği için 4 puan, "Kararsızım" seçeneği için 3 puan, "Katılmıyorum" seçeneği için 2 puan, "Kesinlikle Katılmıyorum" seçeneği için 1 puan olmak üzere değerlendirme yapılmıştır.

Analiz sonunda anket çıktılarından enerji sektöründe görev alan BGYS personelinin kendi kurumlarında ve tüm sektörde yürütülen bilgi güvenliği sistemlerine dair düşüncelerine ulaşılması hedeflenmiştir.

6.3.3. Yönetim anketi

Üçüncü ve son anket, 'Yönetim' anketidir ve üst yönetimin bilgi güvenliği yönetim sistemlerine olan bakış açısından sistemin mevcut durumunun öğrenilebilmesi amacıyla hazırlanmıştır. Anketin çevrimiçi bağlantısı; Bilgi İşlem Dairesi Başkanlığı makamının

desteği ile ETKB Merkez Teşkilat ile Bakanlığın bağlı ve ilgili kuruluşlarında Daire Başkanı ve üstü pozisyonlarda görev alan kişilere iletilmiştir ve 47 yönetici katılım sağlamıştır.

Toplamda 14 adet soruya yer verilen anketin ilk 3 sorusu diğer anketlerde olduğu gibi tanımlama sorularıdır. Öncelikle sektörde ne kadar süredir görev alındığı sorgulanmıştır. Ardından sektör içinde görev aldığı kapsamın seçilmesi istenmiştir. Kapsam için belirlenen cevaplar BGYS sorumlularına yönelik anketteki gibi; elektrik, petrol, doğal gaz, maden, kömür, nükleer ve Bakanlık Merkez Teşkilat olmak üzere sıralanmıştır. Ardından bu kapsamda ne kadar süredir görev yapıldığına dair bir soru sorulmuştur.

Geriye kalan sorularda üst yönetimin bakış açısını ölçmeye yönelik ifadeler yer almaktadır. Bu sorular için beş seçenekli likert tipi olarak düzenlenmiş, cevaplar “Kesinlikle Katılmıyorum”, “Katılmıyorum”, “Kararsızım”, “Katılıyorum” ve “Kesinlikle Katılıyorum” olmak üzere belirlenmiştir. “Kesinlikle Katılıyorum” seçeneği için 5 puan, “Katılıyorum” seçeneği için 4 puan, “Kararsızım” seçeneği için 3 puan, “Katılmıyorum” seçeneği için 2 puan, “Kesinlikle Katılmıyorum” seçeneği için 1 puan olmak üzere değerlendirme yapılmıştır. Anketlerden alınan geri dönüşler sonucunda yapılan analizlerde sektördeki yöneticilerin BGYS çalışmalarına olan bakış açılarının değerlendirilmesi hedeflenmiştir.

7.BULGULAR

Bu bölümde anketlerden elde edilen sonuçlara yer verilmiştir. Üç farklı anket için üç ayrı alt başlık belirlenmiştir ve ilgili başlıkların altında analizin gerçekleştirildiği parametreler değerlendirilerek elde edilen tablolar bulunmaktadır.

7.1. Personel

Personele yönelik anketin analizleri bu bölümde yer almaktadır.

Çizelge 7.1.1. Personel anketi analizi genel tablo

	Kesinlikle Katılmıyorum		Katılmıyorum		Kararsızım		Katılıyorum		Kesinlikle Katılıyorum		Puan		
	f	%	f	%	f	%	f	%	f	%	Toplam	Orta-lama	Standart Sapma
Kurumda, bilgi güvenliği yönetim sistemi iyi şekilde yürütülmektedir.	0	0,0	1	1,8	4	7,0	34	59,6	18	31,6	240,0	4,2	0,6
Bilgi güvenliği yönetim sistemi standardı kapsamında farkındalık eğitimleri alınmaktadır.	0	0,0	1	1,8	7	12,3	32	56,1	17	29,8	236,0	4,1	0,7
Bilgi güvenliği yönetim sistemi ile ilgili verilen eğitimleri yeterlidir.	0	0,0	6	10,5	14	24,6	25	43,9	12	21,1	214,0	3,8	0,9
Bilgi güvenliği yönetim sistemi kapsamında yapılan faaliyetler sayesinde iş süreçleri hızlı ve sağlıklı şekilde yönetilmektedir.	0	0,0	1	1,8	13	22,8	30	52,6	13	22,8	226,0	4,0	0,7
Kurum ve iş yapılan kuruluşların bilgi güvenliği yönetim sistemi sertifikasının olması, bilgi güvenliğini sağlamaktadır.	2	3,5	5	8,8	10	17,5	26	45,6	14	24,6	216,0	3,8	1,0
Bilgi güvenliği yönetim sistemi standardı, bilgi güvenliği konusundaki ihlalleri engellemektedir.	0	0,0	3	5,3	8	14,0	30	52,6	16	28,1	230,0	4,0	0,8
Bilgi güvenliği yönetim sistemi kapsamında yapılan faaliyetler, kurumsal risk analizinin gerçekleştirilmesine katkı sağlamaktadır.	0	0,0	1	1,8	6	10,5	29	50,9	21	36,8	241,0	4,2	0,7
Bilgi güvenliği yönetim sisteminin kalitesini ölçmek adına anketler yapılmaktadır.	0	0,0	9	15,8	11	19,3	25	43,9	12	21,1	211,0	3,7	1,0
Bilgi güvenliği politikası kapsamında meydana gelen değişimler, hali hazırdaki işleyişi etkilememektedir.	0	0,0	6	10,5	19	33,3	21	36,8	11	19,3	208,0	3,6	0,9
Bilgi güvenliği yönetim sistemi politikaları benimsenmekte ve desteklenmektedir.	1	1,8	0	0,0	5	8,8	34	59,6	17	29,8	237,0	4,2	0,7
BGYS birimi çalışanları, bilgi güvenliği yönetim sistemlerinin yürütülmesi sürecinde ekip dışında yer alan personelle iletişim halindedir.	1	1,8	2	3,5	11	19,3	24	42,1	19	33,3	229,0	4,0	0,9

Yukarıda yer verilen Çizelge 7.1'de personele yönelik anketi çözen bütün katılımcıların verdikleri cevapların hesaba katılmasıyla elde edilen sonuçlar görülebilmektedir. Değerlendirmeler soru bazında gerçekleştirilmiştir. Puan sütununda ortalama ve standart sapma değerleri yer almaktadır. Alabileceği en yüksek değer 5 olan ortalama, en düşük 3,6 en fazla ise 4,2 değerini almıştır.

Çizelge 7.1.2. Personel anketi olumlu ve olumsuz yaklaşımı oranları

		f	%
Kurumda, bilgi güvenliği yönetim sistemi iyi şekilde yürütülmektedir.	Olumlu	52	91,2
	Olumsuz	1	1,8
Bilgi güvenliği yönetim sistemi standardı kapsamında farkındalık eğitimleri alınmaktadır.	Olumlu	49	85,9
	Olumsuz	1	1,8
Bilgi güvenliği yönetim sistemi ile ilgili verilen eğitimleri yeterlidir.	Olumlu	37	65
	Olumsuz	6	10,5
Bilgi güvenliği yönetim sistemi kapsamında yapılan faaliyetler sayesinde iş süreçleri hızlı ve sağlıklı şekilde yönetilmektedir.	Olumlu	43	75,4
	Olumsuz	1	1,8
Kurum ve iş yapılan kuruluşların bilgi güvenliği yönetim sistemi sertifikasının olması, bilgi güvenliğini sağlamaktadır.	Olumlu	40	70,2
	Olumsuz	7	12,3
Bilgi güvenliği yönetim sistemi standardı, bilgi güvenliği konusundaki ihlalleri engellemektedir.	Olumlu	46	80,7
	Olumsuz	3	5,3
Bilgi güvenliği yönetim sistemi kapsamında yapılan faaliyetler, kurumsal risk analizinin gerçekleştirilmesine katkı sağlamaktadır.	Olumlu	50	87,7
	Olumsuz	1	1,8
Bilgi güvenliği yönetim sisteminin kalitesini ölçmek adına anketler yapılmaktadır.	Olumlu	37	65
	Olumsuz	9	15,8
Bilgi güvenliği politikası kapsamında meydana gelen değişimler, hali hazırdaki işleyişi etkilememektedir.	Olumlu	32	56,1
	Olumsuz	6	10,5
Bilgi güvenliği yönetim sistemi politikaları benimsenmekte ve desteklenmektedir.	Olumlu	51	89,4
	Olumsuz	1	1,8
BGYS birimi çalışanları, bilgi güvenliği yönetim sistemlerinin yürütülmesi sürecinde ekip dışında yer alan personelle iletişim halindedir.	Olumlu	43	75,4
	Olumsuz	3	5,3

Çizelge 7.2.2'de sorulara verilen yanıtlara göre konuya ilişkin yaklaşımın olumlu ya da olumsuz olduğunu gösterilmektedir. Olumlu yanıtlar için kesinlikle katılıyorum ve katılıyorum, olumsuz yanıtlar için ise kesinlikle katılmıyorum ve katılmıyorum seçenekleri değerlendirmeye alınmıştır. Tablodaki yüzdelik değeri, cevabın tüm cevaplara olan oranının

hesaplanmasıyla belirlenmiştir. Tabloya göre olumlu cevaplar için en düşük yüzdelik değer olan %56,1; personelin bütün sorular için çoğunlukla olumlu yaklaşıma sahip olduğunu göstermektedir.

Genel analizlerden sonra, tanımlamaya yönelik sorulan sorulardan "Hangi birimde görev almaktasınız?" sorusuna istinaden her birim için ayrı analizler gerçekleştirilmiştir.

Çizelge 7.1.3. Bilişim Sistemleri Koordinatörlüğü çalışanlarının cevaplarının analizi

	Kesinlikle Katılmıyorum		Katılmıyorum		Kararsızım		Katılıyorum		Kesinlikle Katılıyorum		Puan		
	f	%	f	%	f	%	f	%	f	%	Toplam	Orta-lama	Standart Sapma
Kurumda, bilgi güvenliği yönetim sistemi iyi şekilde yürütülmektedir.	0	0,0	0	0,0	0	0,0	5	50,0	5	50,0	45	4,50	0,53
Bilgi güvenliği yönetim sistemi standardı kapsamında farkındalık eğitimleri alınmaktadır.	0	0,0	0	0,0	2	20,0	3	30,0	5	50,0	43	4,30	0,82
Bilgi güvenliği yönetim sistemi ile ilgili verilen eğitimleri yeterlidir.	0	0,0	1	10,0	1	10,0	5	50,0	3	30,0	40	4,00	0,94
Bilgi güvenliği yönetim sistemi kapsamında yapılan faaliyetler sayesinde iş süreçleri hızlı ve sağlıklı şekilde yönetilmektedir.	0	0,0	0	0,0	0	0,0	7	70,0	3	30,0	43	4,30	0,48
Kurum ve iş yapılan kuruluşların bilgi güvenliği yönetim sistemi sertifikasının olması, bilgi güvenliğini sağlamaktadır.	0	0,0	0	0,0	2	20,0	4	40,0	4	40,0	42	4,20	0,79
Bilgi güvenliği yönetim sistemi standardı, bilgi güvenliği konusundaki ihlalleri engellemektedir.	0	0,0	0	0,0	0	0,0	5	50,0	5	50,0	45	4,50	0,53
Bilgi güvenliği yönetim sistemi kapsamında yapılan faaliyetler, kurumsal risk analizinin gerçekleştirilmesine katkı sağlamaktadır.	0	0,0	0	0,0	0	0,0	5	50,0	5	50,0	45	4,50	0,53
Bilgi güvenliği yönetim sisteminin kalitesini ölçmek adına anketler yapılmaktadır.	0	0,0	1	10,0	1	10,0	4	40,0	4	40,0	41	4,10	0,99
Bilgi güvenliği politikası kapsamında meydana gelen değişimler, hali hazırdaki işleyişi etkilememektedir.	0	0,0	2	20,0	2	20,0	3	30,0	3	30,0	37	3,70	1,16
Bilgi güvenliği yönetim sistemi politikaları benimsenmekte ve desteklenmektedir.	0	0,0	0	0,0	1	10,0	3	30,0	6	60,0	45	4,50	0,71
BGYS birimi çalışanları, bilgi güvenliği yönetim sistemlerinin yürütülmesi sürecinde ekip dışında yer alan personelle iletişim halindedir.	0	0,0	0	0,0	1	10,0	3	30,0	6	60,0	45	4,50	0,71

Bilişim Sistemleri Koordinatörlüğü'nden ankete on kişi katılım sağlamıştır. Soru bazında cevapların ortalamalarına bakıldığında en yüksek 5 olabilecek olan ortalama değeri için bir soru hariç, diğer sorularda 4 üzeri değer alındığı görülmüştür. Bu soru BGYS kapsamında gerçekleştirilen değişimlerin mevcut duruma olan yansımasının sorgulandığı sorudur ve bu soru için verilen cevapların ortalama değeri 3,7 çıkmıştır.

Çizelge 7.1.4. BT Destek Hizmetleri Koordinatörlüğü çalışanlarının cevaplarının analizi

	Kesinlikle Katılmıyorum		Katılmıyorum		Kararsızım		Katılıyorum		Kesinlikle Katılıyorum		Puan		
	f	%	f	%	f	%	f	%	f	%	Toplam	Orta-lama	Standart Sapma
Kurumda, bilgi güvenliği yönetim sistemi iyi şekilde yürütülmektedir.	0	0,0	0	0,0	1	12,5	6	75,0	1	12,5	32	4,00	0,53
Bilgi güvenliği yönetim sistemi standardı kapsamında farkındalık eğitimleri alınmaktadır.	0	0,0	0	0,0	1	12,5	7	87,5	0	0,0	31	3,88	0,35
Bilgi güvenliği yönetim sistemi ile ilgili verilen eğitimleri yeterlidir.	0	0,0	1	12,5	5	62,5	2	25,0	0	0,0	25	3,13	0,64
Bilgi güvenliği yönetim sistemi kapsamında yapılan faaliyetler sayesinde iş süreçleri hızlı ve sağlıklı şekilde yönetilmektedir.	0	0,0	0	0,0	3	37,5	5	62,5	0	0,0	29	3,63	0,52
Kurum ve iş yapılan kuruluşların bilgi güvenliği yönetim sistemi sertifikasının olması, bilgi güvenliğini sağlamaktadır.	0	0,0	1	12,5	4	50,0	2	25,0	1	12,5	27	3,38	0,92
Bilgi güvenliği yönetim sistemi standardı, bilgi güvenliği konusundaki ihlalleri engellemektedir.	0	0,0	1	12,5	2	25,0	4	50,0	1	12,5	29	3,63	0,92
Bilgi güvenliği yönetim sistemi kapsamında yapılan faaliyetler, kurumsal risk analizinin gerçekleştirilmesine katkı sağlamaktadır.	0	0,0	0	0,0	1	12,5	5	62,5	2	25,0	33	4,13	0,64
Bilgi güvenliği yönetim sisteminin kalitesini ölçmek adına anketler yapılmaktadır.	0	0,0	1	12,5	2	25,0	5	62,5	0	0,0	28	3,50	0,76
Bilgi güvenliği politikası kapsamında meydana gelen değişimler, hali hazırdaki işleyişi etkilememektedir.	0	0,0	1	12,5	4	50,0	3	37,5	0	0,0	26	3,25	0,71
Bilgi güvenliği yönetim sistemi politikaları benimsenmekte ve desteklenmektedir.	0	0,0	0	0,0	0	0,0	6	75,0	2	25,0	34	4,25	0,46
BGYS birimi çalışanları, bilgi güvenliği yönetim sistemlerinin yürütülmesi sürecinde ekip dışında yer alan personelle iletişim halindedir.	0	0,0	0	0,0	2	25,0	5	62,5	1	12,5	31	3,88	0,64

BT Destek Hizmetleri Koordinatörlüğü personeli tarafından verilen cevapların analizi Çizelge 7.1.4.'de gösterilmiştir. Bu birimden toplam 8 kişi ankete katılım sağlamıştır.

En düşük ortalama değeri olan 3,13; BGYS hususundaki eğitimlerin yeterli olup olmadığının sorgulandığı soruda görülmektedir. Toplamda 5 adet soruya olumsuz cevap verilmiştir. Olumsuz cevap verilen sorulardan 2 tanesi (5. ve 6. sorular) BGYS ile ilgili eleştiri olarak değerlendirilebilirken diğer 3 soru BGYS'nin kurum içinde yürütülmesine yöneliktir.

Çizelge 7.1.5. BT Personel ve Eğitim Müdürlüğü çalışanlarının cevaplarının analizi

	Kesinlikle Katılmıyorum		Katılmıyorum		Kararsızım		Katılıyorum		Kesinlikle Katılıyorum		Puan		
	f	%	f	%	f	%	f	%	f	%	Toplam	Orta-lama	Standart Sapma
Kurumda, bilgi güvenliği yönetim sistemi iyi şekilde yürütülmektedir.	0	0,0	0	0,0	0	0,0	3	100,0	0	0,0	12	4,00	0,00
Bilgi güvenliği yönetim sistemi standardı kapsamında farkındalık eğitimleri alınmaktadır.	0	0,0	0	0,0	0	0,0	3	100,0	0	0,0	12	4,00	0,00
Bilgi güvenliği yönetim sistemi ile ilgili verilen eğitimleri yeterlidir.	0	0,0	0	0,0	0	0,0	3	100,0	0	0,0	12	4,00	0,00
Bilgi güvenliği yönetim sistemi kapsamında yapılan faaliyetler sayesinde iş süreçleri hızlı ve sağlıklı şekilde yönetilmektedir.	0	0,0	0	0,0	0	0,0	3	100,0	0	0,0	12	4,00	0,00
Kurum ve iş yapılan kuruluşların bilgi güvenliği yönetim sistemi sertifikasının olması, bilgi güvenliğini sağlamaktadır.	0	0,0	0	0,0	0	0,0	3	100,0	0	0,0	12	4,00	0,00
Bilgi güvenliği yönetim sistemi standardı, bilgi güvenliği konusundaki ihlalleri engellemektedir.	0	0,0	0	0,0	0	0,0	3	100,0	0	0,0	12	4,00	0,00
Bilgi güvenliği yönetim sistemi kapsamında yapılan faaliyetler, kurumsal risk analizinin gerçekleştirilmesine katkı sağlamaktadır.	0	0,0	0	0,0	1	33,3	2	66,7	0	0,0	11	3,67	0,58
Bilgi güvenliği yönetim sisteminin kalitesini ölçmek adına anketler yapılmaktadır.	0	0,0	0	0,0	0	0,0	3	100,0	0	0,0	12	4,00	0,00
Bilgi güvenliği politikası kapsamında meydana gelen değişimler, hali hazırdaki işleyişi etkilememektedir.	0	0,0	0	0,0	1	33,3	2	66,7	0	0,0	11	3,67	0,58
Bilgi güvenliği yönetim sistemi politikaları benimsenmekte ve desteklenmektedir.	0	0,0	0	0,0	1	33,3	2	66,7	0	0,0	11	3,67	0,58
BGYS birimi çalışanları, bilgi güvenliği yönetim sistemlerinin yürütülmesi sürecinde ekip dışında yer alan personelle iletişim halindedir.	0	0,0	0	0,0	0	0,0	3	100,0	0	0,0	12	4,00	0,00

Yukarıdaki Çizelge 7.1.5. isimli tabloda analizi gösterilen BT Personel ve Eğitim Müdürlüğü'nden 3 çalışan ankete katılım sağlamıştır. Katılımcılar soruların birçoğunda "Katılıyorum" seçeneğini işaretlemiştir. Üç soruda ise "Kararsızım" seçeneğini işaretleyen

birer personelin olduğu görülmektedir. Ayrıca bu birimde personeller arası fikir birliğinin sağlandığı yani en düşük standart sapma değerine sahip biriminin olduğu ortaya koyulmuştur. Ancak elbette bu birimde yer alan personel sayısının az olduğundan dolayı böyle bir sonucun çıkma durumu da değerlendirilmesi gereken bir konudur.

Çizelge 7.1.6. Proje Yönetimi Koordinatörlüğü çalışanlarının cevaplarının analizi

	Kesinlikle Katılmıyorum		Katılmıyorum		Kararsızım		Katılıyorum		Kesinlikle Katılıyorum		Puan		
	f	%	f	%	f	%	f	%	f	%	Toplam	Orta-lama	Standart Sapma
Kurumda, bilgi güvenliği yönetim sistemi iyi şekilde yürütülmektedir.	0	0,0	0	0,0	0	0,0	3	75,0	1	25,0	17	4,25	0,50
Bilgi güvenliği yönetim sistemi standardı kapsamında farkındalık eğitimleri alınmaktadır.	0	0,0	0	0,0	0	0,0	3	75,0	1	25,0	17	4,25	0,50
Bilgi güvenliği yönetim sistemi ile ilgili verilen eğitimleri yeterlidir.	0	0,0	0	0,0	2	50,0	1	25,0	1	25,0	15	3,75	0,96
Bilgi güvenliği yönetim sistemi kapsamında yapılan faaliyetler sayesinde iş süreçleri hızlı ve sağlıklı şekilde yönetilmektedir.	0	0,0	0	0,0	0	0,0	3	75,0	1	25,0	17	4,25	0,50
Kurum ve iş yapılan kuruluşların bilgi güvenliği yönetim sistemi sertifikasının olması, bilgi güvenliğini sağlamaktadır.	0	0,0	2	50,0	0	0,0	1	25,0	1	25,0	13	3,25	1,50
Bilgi güvenliği yönetim sistemi standardı, bilgi güvenliği konusundaki ihlalleri engellemektedir.	0	0,0	1	25,0	1	25,0	1	25,0	1	25,0	14	3,50	1,29
Bilgi güvenliği yönetim sistemi kapsamında yapılan faaliyetler, kurumsal risk analizinin gerçekleştirilmesine katkı sağlamaktadır.	0	0,0	0	0,0	0	0,0	2	50,0	2	50,0	18	4,50	0,58
Bilgi güvenliği yönetim sisteminin kalitesini ölçmek adına anketler yapılmaktadır.	0	0,0	1	25,0	0	0,0	2	50,0	1	25,0	15	3,75	1,26
Bilgi güvenliği politikası kapsamında meydana gelen değişimler, hali hazırdaki işleyişi etkilememektedir.	0	0,0	1	25,0	1	25,0	1	25,0	1	25,0	14	3,50	1,29
Bilgi güvenliği yönetim sistemi politikaları benimsenmekte ve desteklenmektedir.	0	0,0	0	0,0	0	0,0	3	75,0	1	25,0	17	4,25	0,50
BGYS birimi çalışanları, bilgi güvenliği yönetim sistemlerinin yürütülmesi sürecinde ekip dışında yer alan personelle iletişim halindedir.	0	0,0	1	25,0	0	0,0	2	50,0	1	25,0	15	3,75	1,26

Proje Yönetimi Koordinatörlüğü'nden ankete katılan 4 kişinin verdiği cevapların analizi Çizelge 7.1.6.'da gösterilmiştir. Anketi çözen personellerin hem BGYS'nin temel amaçları

ile ilgili hem de kurum içerisinde yürütülen BGYS çalışmaları ile ilgili olumsuz düşüncelere sahip oldukları görülmektedir.

Bir diğer analiz ise Çizelge 7.1.7.'de gösterilen, 21 katılımcı ile birimler arasında ankete en çok katılım sağlayan birim olan Siber Güvenlik ve Bilişim Ağları Koordinatörlüğü personelinin cevaplarının yer aldığı analizdir.

Çizelge 7.1.7. Siber Güvenlik ve Bilişim Ağları Koordinatörlüğü çalışanlarının cevaplarının analizi

	Kesinlikle Katılmıyorum		Katılmıyorum		Kararsızım		Katılıyorum		Kesinlikle Katılıyorum		Puan		
	f	%	f	%	f	%	f	%	f	%	Toplam	Orta-lama	Standart Sapma
Kurumda, bilgi güvenliği yönetim sistemi iyi şekilde yürütülmektedir.	0	0,0	1	4,8	2	9,5	9	42,9	9	42,9	89	4,24	0,83
Bilgi güvenliği yönetim sistemi standardı kapsamında farkındalık eğitimleri alınmaktadır.	0	0,0	1	4,8	3	14,3	7	33,3	10	47,6	89	4,24	0,89
Bilgi güvenliği yönetim sistemi ile ilgili verilen eğitimleri yeterlidir.	0	0,0	4	19,0	3	14,3	7	33,3	7	33,3	80	3,81	1,12
Bilgi güvenliği yönetim sistemi kapsamında yapılan faaliyetler sayesinde iş süreçleri hızlı ve sağlıklı şekilde yönetilmektedir.	0	0,0	1	4,8	7	33,3	5	23,8	8	38,1	83	3,95	0,97
Kurum ve iş yapılan kuruluşların bilgi güvenliği yönetim sistemi sertifikasının olması, bilgi güvenliğini sağlamaktadır.	2	9,5	1	4,8	2	9,5	8	38,1	8	38,1	82	3,90	1,26
Bilgi güvenliği yönetim sistemi standardı, bilgi güvenliği konusundaki ihlalleri engellemektedir.	0	0,0	1	4,8	5	23,8	8	38,1	7	33,3	84	4,00	0,89
Bilgi güvenliği yönetim sistemi kapsamında yapılan faaliyetler, kurumsal risk analizinin gerçekleştirilmesine katkı sağlamaktadır.	0	0,0	1	4,8	3	14,3	7	33,3	10	47,6	89	4,24	0,89
Bilgi güvenliği yönetim sisteminin kalitesini ölçmek adına anketler yapılmaktadır.	0	0,0	4	19,0	4	19,0	6	28,6	7	33,3	79	3,76	1,14
Bilgi güvenliği politikası kapsamında meydana gelen değişimler, hali hazırdaki işleyişi etkilememektedir.	0	0,0	2	9,5	4	19,0	8	38,1	7	33,3	83	3,95	0,97
Bilgi güvenliği yönetim sistemi politikaları benimsenmekte ve desteklenmektedir.	1	4,8	0	0,0	3	14,3	10	47,6	7	33,3	85	4,05	0,97
BGYS birimi çalışanları, bilgi güvenliği yönetim sistemlerinin yürütülmesi sürecinde ekip dışında yer alan personelle iletişim halindedir.	1	4,8	0	0,0	3	14,3	6	28,6	11	52,4	89	4,24	1,04

Yukarıdaki tabloda görülebileceği üzere bazı sorulara “Kesinlikle Katılmıyorum” cevabını veren personeller bulunmaktadır. Tüm birimlerin sonuçları incelendikten sonra bu seçeneğin yalnızca Siber Güvenlik ve Bilişim Ağları Koordinatörlüğü bünyesinde çalışan personel tarafından işaretlendiği tespit edilmiştir. Standart sapma değeri 1,26 olmak üzere en yüksek olan soru aynı zamanda “Kesinlikle Katılmıyorum” seçeneğini tercih eden 2 personelin olduğu sorudur. Buna rağmen soru bazında ortalama alındığında en düşük ortalama değerinin %3,76 olduğu görülebilmektedir.

Çizelge 7.1.8. Yazılım Koordinatörlüğü çalışanlarının cevaplarının analizi

	Kesinlikle Katılmıyorum		Katılmıyorum		Kararsızım		Katılıyorum		Kesinlikle Katılıyorum		Puan		
	f	%	f	%	f	%	f	%	f	%	Toplam	Orta-lama	Standart Sapma
Kurumda, bilgi güvenliği yönetim sistemi iyi şekilde yürütülmektedir.	0	0,0	0	0,0	1	9,1	8	72,7	2	18,2	45	4,09	0,54
Bilgi güvenliği yönetim sistemi standardı kapsamında farkındalık eğitimleri alınmaktadır.	0	0,0	0	0,0	1	9,1	9	81,8	1	9,1	44	4,00	0,45
Bilgi güvenliği yönetim sistemi ile ilgili verilen eğitimleri yeterlidir.	0	0,0	0	0,0	3	27,3	7	63,6	1	9,1	42	3,82	0,60
Bilgi güvenliği yönetim sistemi kapsamında yapılan faaliyetler sayesinde iş süreçleri hızlı ve sağlıklı şekilde yönetilmektedir.	0	0,0	0	0,0	3	27,3	7	63,6	1	9,1	42	3,82	0,60
Kurum ve iş yapılan kuruluşların bilgi güvenliği yönetim sistemi sertifikasının olması, bilgi güvenliğini sağlamaktadır.	0	0,0	1	9,1	2	18,2	8	72,7	0	0,0	40	3,64	0,67
Bilgi güvenliği yönetim sistemi standardı, bilgi güvenliği konusundaki ihlalleri engellemektedir.	0	0,0	0	0,0	0	0,0	9	81,8	2	18,2	46	4,18	0,40
Bilgi güvenliği yönetim sistemi kapsamında yapılan faaliyetler, kurumsal risk analizinin gerçekleştirilmesine katkı sağlamaktadır.	0	0,0	0	0,0	1	9,1	8	72,7	2	18,2	45	4,09	0,54
Bilgi güvenliği yönetim sisteminin kalitesini ölçmek adına anketler yapılmaktadır.	0	0,0	2	18,2	4	36,4	5	45,5	0	0,0	36	3,27	0,79
Bilgi güvenliği politikası kapsamında meydana gelen değişimler, hali hazırdaki işleyişi etkilememektedir.	0	0,0	0	0,0	7	63,6	4	36,4	0	0,0	37	3,36	0,50
Bilgi güvenliği yönetim sistemi politikaları benimsenmekte ve desteklenmektedir.	0	0,0	0	0,0	0	0,0	10	90,9	1	9,1	45	4,09	0,30
BGYS birimi çalışanları, bilgi güvenliği yönetim sistemlerinin yürütülmesi sürecinde ekip dışında yer alan personelle iletişim halindedir.	0	0,0	1	9,1	5	45,5	5	45,5	0	0,0	37	3,36	0,67

Yazılım Koordinatörlüğü'nden 11 kişi ankete katılım sağlamıştır. Anketin analizi ise yukarıda, Çizelge 7.1.8.'de gösterilmektedir. Diğer birimlerle karşılaştırıldığında en yüksek oranda çekimser oy kullanan personelin Yazılım Koordinatörlüğü'nde olduğu belirlenmiştir.

Çizelge 7.1.9. Personelin görev süresine göre olumlu ve olumsuz bakış açısının analizi

		Ne kadar süredir bu birimde görev almaktasınız?							
		0-5 Yıl		6-10 Yıl		10 Yıldan Fazla		Total	
		f	%	f	%	f	%	f	%
Kurumda, bilgi güvenliği yönetim sistemi iyi şekilde yürütülmektedir.	Olumlu	46	88,5	3	5,8	3	5,8	52	100,0
	Olumsuz	1	100,0	0	0,0	0	0,0	1	100,0
Bilgi güvenliği yönetim sistemi standardı kapsamında farkındalık eğitimleri alınmaktadır.	Olumlu	43	87,8	3	6,1	3	6,1	49	100,0
	Olumsuz	1	100,0	0	0,0	0	0,0	1	100,0
Bilgi güvenliği yönetim sistemi ile ilgili verilen eğitimleri yeterlidir.	Olumlu	33	89,2	2	5,4	2	5,4	37	100,0
	Olumsuz	4	66,7	1	16,7	1	16,7	6	100,0
Bilgi güvenliği yönetim sistemi kapsamında yapılan faaliyetler sayesinde iş süreçleri hızlı ve sağlıklı şekilde yönetilmektedir.	Olumlu	37	86,0	3	7,0	3	7,0	43	100,0
	Olumsuz	1	100,0	0	0,0	0	0,0	1	100,0
Kurum ve iş yapılan kuruluşların bilgi güvenliği yönetim sistemi sertifikasının olması, bilgi güvenliğini sağlamaktadır.	Olumlu	35	87,5	3	7,5	2	5,0	40	100,0
	Olumsuz	6	85,7	0	0,0	1	14,3	7	100,0
Bilgi güvenliği yönetim sistemi standardı, bilgi güvenliği konusundaki ihlalleri engellemektedir.	Olumlu	42	91,3	2	4,3	2	4,3	46	100,0
	Olumsuz	2	66,7	0	0,0	1	33,3	3	100,0
Bilgi güvenliği yönetim sistemi kapsamında yapılan faaliyetler, kurumsal risk analizinin gerçekleştirilmesine katkı sağlamaktadır.	Olumlu	44	88,0	3	6,0	3	6,0	50	100,0
	Olumsuz	1	100,0	0	0,0	0	0,0	1	100,0
Bilgi güvenliği yönetim sisteminin kalitesini ölçmek adına anketler yapılmaktadır.	Olumlu	34	91,9	2	5,4	1	2,7	37	100,0
	Olumsuz	8	88,9	1	11,1	0	0,0	9	100,0
Bilgi güvenliği politikası kapsamında meydana gelen değişimler, hali hazırdaki işleyişi etkilememektedir.	Olumlu	28	87,5	2	6,3	2	6,3	32	100,0
	Olumsuz	5	83,3	1	16,7	0	0,0	6	100,0
Bilgi güvenliği yönetim sistemi politikaları benimsenmekte ve desteklenmektedir.	Olumlu	45	88,2	3	5,9	3	5,9	51	100,0
	Olumsuz	1	100,0	0	0,0	0	0,0	1	100,0
BGYS birimi çalışanları, bilgi güvenliği yönetim sistemlerinin yürütülmesi sürecinde ekip dışında yer alan personelle iletişim halindedir.	Olumlu	39	90,7	3	7,0	1	2,3	43	100,0
	Olumsuz	3	100,0	0	0,0	0	0,0	3	100,0

Personele yönelik ankette, katılımcının yer aldığı birimde ne kadar süredir görev yaptığı sorusu da yer almaktadır. Bu sorunun sorulmasındaki amaç tecrübenin BGYS için bakış açısında bir değişiklik oluşturma ihtimalini değerlendirmekti. Ancak 0-5 yıl arası deneyimi olan personel seçeneğinde yığılma olması sebebiyle değerlendirmenin objektif olmayacağı kanaatine varılmıştır.

7.2. BGYS Çalışanları

Daha önce ifade edildiği üzere "BGYS Çalışanları" anketi; ETKB Merkez Teşkilattaki BGYS birimi personeli ile kendi birimlerinin BGYS sorumlusu olan personellerin ayrıca bağlı ve ilgili kuruluşlardaki BGYS birimi personelinin katılımına sunulmuştur.

Çizelge 7.2.1. BGYS çalışanları anketi genel tablo

	Kesinlikle Katılmıyorum		Katılmıyorum		Kararsızım		Katılıyorum		Kesinlikle Katılıyorum		Puan		
	f	%	f	%	f	%	f	%	f	%	Toplam	Ort.	S.Sapma
Bilgi güvenliği yönetim sistemi birimi üyeleri, sistemin kurulumu ve yürütülmesi açısından sayıca yeterlidir.	1	1,3	12	15,6	17	22,1	32	41,6	15	19,5	279,0	3,6	1,0
Bilgi güvenliği yönetim sisteminin kurulması ve yürütülmesi için kurum personeli yeterli donanıma sahiptir.	0	0,0	14	18,2	15	19,5	37	48,1	11	14,3	276,0	3,6	1,0
Bilgi güvenliği yönetim sisteminin kurulması için danışmanlık hizmeti alınmıştır.	1	1,3	6	7,8	24	31,2	31	40,3	15	19,5	284,0	3,7	0,9
Bilgi güvenliği yönetim sisteminde süreçlerin düzgün yürütülebilmesi için BGYS Birimi personeli eğitim almıştır.	1	1,3	6	7,8	12	15,6	35	45,5	23	29,9	304,0	3,9	0,9
Bilgi güvenliği yönetim sistemi bütün kurum personeli ile iş birliği içerisinde yürütülmektedir.	3	3,9	6	7,8	14	18,2	38	49,4	16	20,8	289,0	3,8	1,0
Bilgi güvenliği yönetim sistemi politikaları herkes tarafından anlaşılır düzeyde hazırlanarak kurum personeliyle birlikte tüm iç ve dış paydaşlara bildirilmektedir.	0	0,0	3	3,9	10	13,0	48	62,3	16	20,8	308,0	4,0	0,7
Bilgi güvenliği yönetim sistemi politikaları kurum bünyesindeki bütün çalışanlar tarafından benimsenmektedir.	0	0,0	14	18,2	21	27,3	32	41,6	10	13,0	269,0	3,5	0,9
Bilgi güvenliği politikası kapsamında meydana gelen değişimler, çalışanlar tarafından hali hazırda işleyen sisteme tehdit olarak algılanmamaktadır.	0	0,0	11	14,3	23	29,9	33	42,9	10	13,0	273,0	3,5	0,9
Bilgi güvenliği standartlarına sahip olmak kurumsal bilgi güvenliğini sağlamaktadır.	0	0,0	2	2,6	8	10,4	43	55,8	24	31,2	320,0	4,2	0,7
Bilgi güvenliği standartları sayesinde, kurum içi ve kurum dışındaki kritik bilgi güvenliği gereksinimleri karşılanmaktadır.	0	0,0	1	1,3	9	11,7	48	62,3	19	24,7	316,0	4,1	0,6
Bilgi güvenliği sertifikasyonu sonrası süreçte, kurum personeli yeni kurallara uyum sağlamakta zorlanmamıştır.	0	0,0	11	14,3	24	31,2	34	44,2	8	10,4	270,0	3,5	0,9
BGYS Birimi, bilgi güvenliği yönetim sistemlerinin yürütülmesi sürecinde ekip dışında yer alan personelle iletişim halindedir.	0	0,0	6	7,8	11	14,3	48	62,3	12	15,6	297,0	3,9	0,8

Çizelge 7.2.1. BGYS çalışanları anketi genel sonuçlar

	Kesinlikle Katılmıyorum		Katılmıyorum		Kararsızım		Katılıyorum		Kesinlikle Katılıyorum		Puan		
	f	%	f	%	f	%	f	%	f	%	Toplam	Ort.	S.Sapma
Bilgi güvenliği yönetim sisteminin yürütülmesinde bütün birimler eşgüdümlü olarak dahil olmaktadır.	1	1,3	11	14,3	18	23,4	35	45,5	12	15,6	277,0	3,6	1,0
Bilgi güvenliği yönetim sistemi kapsamında, sürekli iyileştirmeler ve güncellemeler yapılmaktadır.	0	0,0	3	3,9	12	15,6	44	57,1	18	23,4	308,0	4,0	0,7
Bilgi güvenliği yönetim sisteminin kalitesini ölçmek adına yapılan faaliyetlerin çıktıları doğrultusunda gerekli aksiyonlar alınmaktadır.	0	0,0	1	1,3	13	16,9	49	63,6	14	18,2	307,0	4,0	0,6
Kurumda bilgi güvenliği standardı belgesine sahip olmadan önce bilgi güvenliği politikaları mevcut değildi.	2	2,6	7	9,1	36	46,8	26	33,8	6	7,8	258,0	3,4	0,9
Kurumda bilgi güvenliği standardı belgesi, belgeye sahip olmadan önceki bilgi güvenliği politikalarında bir değişikliğe sebep olmuştur.	0	0,0	2	2,6	23	29,9	40	51,9	12	15,6	293,0	3,8	0,7
Bilgi güvenliği yönetim sistemi kurulduktan sonra, öncesine göre güvenlik seviyesinde artış olmuştur.	1	1,3	0	0,0	8	10,4	47	61,0	21	27,3	318,0	4,1	0,7
Bilgi güvenliği yönetim sistemi kurulduktan sonra, öncesine göre kuruma yönelik siber saldırılarda azalma olmuştur.	1	1,3	4	5,2	30	39,0	27	35,1	15	19,5	282,0	3,7	0,9
Bilgi güvenliği yönetim sistemi kurulduktan sonra, öncesine göre kişisel ve kurumsal veri ihlallerinde azalma olmuştur.	0	0,0	0	0,0	17	22,1	42	54,5	18	23,4	309,0	4,0	0,7

Çizelge 7.2.2.'de enerji sektöründe, kurumlarında BGYS'nin yürütülmesi hususundaki faaliyetlerde görev alan personele yönelik ankete katılan kişilerin verdiği cevapların analizi görülmektedir. Analiz ile ilgili değerlere bakıldığında çoğunlukla olumlu yönde cevapların alındığı söylenebilmektedir.

Tablo genel hatlarıyla incelendiğinde en fazla 5 olabilecek ortalamanın aldığı en küçük değerin 3,4 olduğu görülmektedir. Bu değere sahip olan soruda kurumun ISO/IEC 27001 gibi bir bilgi güvenliği standardı belgesine sahip olmadan önce bilgi güvenliğinin korunmasına dair politikaların varlığı sorgulanmıştır. Burada büyük ölçüde çekimser oy kullanıldığı görülebilmektedir. Yanıt olarak doğrudan olumlu ya da olumsuz cevap verilmemesinin nedeninin bilgi eksikliği olduğu düşünülmektedir. Bu durumun personelin kurumda BGYS belgelendirmesinden sonra göreve başlamasından ve daha önceki işleyiş hakkında bilgi sahibi olmamasından kaynaklanması ihtimali değerlendirilmektedir.

Çizelge 7.2.2. BGYS Çalışanları anketi olumlu ve olumsuz cevapların analizi

		f	%
Bilgi güvenliği yönetim sistemi birimi üyeleri, sistemin kurulumu ve yürütülmesi açısından sayıca yeterlidir.	Olumlu	47	61,1
	Olumsuz	13	16,9
Bilgi güvenliği yönetim sisteminin kurulması ve yürütülmesi için kurum personeli yeterli donanıma sahiptir.	Olumlu	48	62,4
	Olumsuz	14	18,2
Bilgi güvenliği yönetim sisteminin kurulması için danışmanlık hizmeti alınmıştır.	Olumlu	46	59,8
	Olumsuz	7	9,1
Bilgi güvenliği yönetim sisteminde süreçlerin düzgün yürütülebilmesi için BGYS Birimi personeli eğitim almıştır.	Olumlu	58	75,4
	Olumsuz	7	9,1
Bilgi güvenliği yönetim sistemi bütün kurum personeli ile iş birliği içerisinde yürütülmektedir.	Olumlu	54	70,2
	Olumsuz	9	11,7
Bilgi güvenliği yönetim sistemi politikaları herkes tarafından anlaşılır düzeyde hazırlanarak kurum personeliyle birlikte tüm iç ve dış paydaşlara bildirilmektedir.	Olumlu	64	83,1
	Olumsuz	3	3,9
Bilgi güvenliği yönetim sistemi politikaları kurum bünyesindeki bütün çalışanlar tarafından benimsenmektedir.	Olumlu	42	54,6
	Olumsuz	14	18,2
Bilgi güvenliği politikası kapsamında meydana gelen değişimler, çalışanlar tarafından hali hazırda işleyen sisteme tehdit olarak algılanmamaktadır.	Olumlu	43	55,9
	Olumsuz	11	14,3
Bilgi güvenliği standartlarına sahip olmak kurumsal bilgi güvenliğini sağlamaktadır.	Olumlu	67	87
	Olumsuz	2	2,6
Bilgi güvenliği standartları sayesinde, kurum içi ve kurum dışındaki kritik bilgi güvenliği gereksinimleri karşılanmaktadır.	Olumlu	67	87
	Olumsuz	1	1,3
Bilgi güvenliği sertifikasyonu sonrası süreçte, kurum personeli yeni kurallara uyum sağlamakta zorlanmamıştır.	Olumlu	42	54,6
	Olumsuz	11	14,3
BGYS Birimi, bilgi güvenliği yönetim sistemlerinin yürütülmesi sürecinde ekip dışında yer alan personelle iletişim halindedir.	Olumlu	60	77,9
	Olumsuz	6	7,8
Bilgi güvenliği yönetim sisteminin yürütülmesinde bütün birimler eşgüdümlü olarak dahil olmaktadır.	Olumlu	47	61,1
	Olumsuz	12	15,6
Bilgi güvenliği yönetim sistemi kapsamında, sürekli iyileştirmeler ve güncellemeler yapılmaktadır.	Olumlu	62	80,5
	Olumsuz	3	3,9
Bilgi güvenliği yönetim sisteminin kalitesini ölçmek adına yapılan faaliyetlerin çıktıları doğrultusunda gerekli aksiyonlar alınmaktadır.	Olumlu	63	81,8
	Olumsuz	1	1,3
Kurumda bilgi güvenliği standardı belgesine sahip olmadan önce bilgi güvenliği politikaları mevcut değildi.	Olumlu	32	40,8
	Olumsuz	9	11,7

Çizelge 7.2.2. BGYS Çalışanları anketi olumlu ve olumsuz cevapların analizi (devam)

		f	%
Kurumda bilgi güvenliği standardı belgesi, belgeye sahip olmadan önceki bilgi güvenliği politikalarında bir değişikliğe sebep olmuştur.	Olumlu	52	67,5
	Olumsuz	2	2,6
Bilgi güvenliği yönetim sistemi kurulduktan sonra, öncesine göre güvenlik seviyesinde artış olmuştur.	Olumlu	68	88,3
	Olumsuz	1	1,3
Bilgi güvenliği yönetim sistemi kurulduktan sonra, öncesine göre kuruma yönelik siber saldırılarda azalma olmuştur.	Olumlu	42	54,6
	Olumsuz	5	6,5
Bilgi güvenliği yönetim sistemi kurulduktan sonra, öncesine göre kişisel ve kurumsal veri ihlallerinde azalma olmuştur.	Olumlu	60	77,9
	Olumsuz	0	0

Çizelge 7.2.2.'de BGYS çalışanlarına yönelik ankette bulunan olumlu ve olumsuz cevapların analizleri yer almaktadır. Soruların tamamında olumlu yaklaşımın hâkim olduğu görülebilmektedir. Bu ankete katılan 77 personel bulunmaktadır. Çizelge 7.2.1. ve Çizelge 7.2.2. incelendiğinde çok sayıda çekimser yanıt veren katılımcı olduğu anlaşılmaktadır.

Çizelge 7.2.2'ye bakıldığında olumsuz yanıt verilmemiş tek bir soru göze çarpmaktadır. Bu soru kurumda bilgi güvenliği yönetim sistemi kurulduktan sonra, öncesine göre kişisel ve kurumsal veri ihlallerinde azalma olduğunu ifade eden sorudur. Soru için verilen olumlu yanıtların oranının 77,9% olduğu görülmektedir. Geriye kalan 22,1%'lik oran ise kararsız oldukları yönünde oy kullanan kişilerin cevaplarından oluşmaktadır.

Çizelge 7.2.3. Doğal gaz sektöründeki BGYS çalışanlarının cevaplarının analizi

	Kesinlikle Katılmıyorum		Katılmıyorum		Kararsızım		Katılıyorum		Kesinlikle Katılıyorum		Puan		
	f	%	f	%	f	%	f	%	f	%	Toplam	Ort.	S.Sapma
Bilgi güvenliği yönetim sistemi birimi üyeleri, sistemin kurulumu ve yürütülmesi açısından sayıca yeterlidir.	0	0,0	0	0,0	0	0,0	3	75,0	1	25,0	17,0	4,3	0,5
Bilgi güvenliği yönetim sisteminin kurulması ve yürütülmesi için kurum personeli yeterli donanıma sahiptir.	0	0,0	0	0,0	0	0,0	3	75,0	1	25,0	17,0	4,3	0,5
Bilgi güvenliği yönetim sisteminin kurulması için danışmanlık hizmeti alınmıştır.	0	0,0	1	25,0	0	0,0	2	50,0	1	25,0	15,0	3,8	1,3
Bilgi güvenliği yönetim sisteminde süreçlerin düzgün yürütülebilmesi için BGYS Birimi personeli eğitim almıştır.	0	0,0	0	0,0	0	0,0	3	75,0	1	25,0	17,0	4,3	0,5
Bilgi güvenliği yönetim sistemi bütün kurum personeli ile iş birliği içerisinde yürütülmektedir.	0	0,0	1	25,0	0	0,0	3	75,0	0	0,0	14,0	3,5	1,0

Çizelge 7.2.3. Doğal gaz sektöründeki BGYS çalışanlarının cevaplarının analizi (devam)

	Kesinlikle Katılmıyorum		Katılmıyorum		Kararsızım		Katılıyorum		Kesinlikle Katılıyorum		Puan		
	f	%	f	%	f	%	f	%	f	%	Toplam	Ort.	S.Sapma
Bilgi güvenliği yönetim sistemi politikaları herkes tarafından anlaşılır düzeyde hazırlanarak kurum personeliyle birlikte tüm iç ve dış paydaşlara bildirilmektedir.	0	0,0	0	0,0	0	0,0	4	100,0	0	0,0	16,0	4,0	0,0
Bilgi güvenliği yönetim sistemi politikaları kurum bünyesindeki bütün çalışanlar tarafından benimsenmektedir.	0	0,0	1	25,0	1	25,0	2	50,0	0	0,0	13,0	3,3	1,0
Bilgi güvenliği politikası kapsamında meydana gelen değişimler, çalışanlar tarafından hali hazırda işleyen sisteme tehdit olarak algılanmamaktadır.	0	0,0	1	25,0	0	0,0	3	75,0	0	0,0	14,0	3,5	1,0
Bilgi güvenliği standartlarına sahip olmak kurumsal bilgi güvenliğini sağlamaktadır.	0	0,0	0	0,0	0	0,0	4	100,0	0	0,0	16,0	4,0	0,0
Bilgi güvenliği standartları sayesinde, kurum içi ve kurum dışındaki kritik bilgi güvenliği gereksinimleri karşılanmaktadır.	0	0,0	0	0,0	0	0,0	4	100,0	0	0,0	16,0	4,0	0,0
Bilgi güvenliği sertifikasyonu sonrası süreçte, kurum personeli yeni kurallara uyum sağlamakta zorlanmamıştır.	0	0,0	1	25,0	1	25,0	2	50,0	0	0,0	13,0	3,3	1,0
BGYS Birimi, bilgi güvenliği yönetim sistemlerinin yürütülmesi sürecinde ekip dışında yer alan personelle iletişim halindedir.	0	0,0	0	0,0	2	50,0	2	50,0	0	0,0	14,0	3,5	0,6
Bilgi güvenliği yönetim sisteminin yürütülmesinde bütün birimler eşgüdümlü olarak dahil olmaktadır.	0	0,0	0	0,0	1	25,0	3	75,0	0	0,0	15,0	3,8	0,5
Bilgi güvenliği yönetim sistemi kapsamında, sürekli iyileştirmeler ve güncellemeler yapılmaktadır.	0	0,0	0	0,0	0	0,0	3	75,0	1	25,0	17,0	4,3	0,5
Bilgi güvenliği yönetim sisteminin kalitesini ölçmek adına yapılan faaliyetlerin çıktıları doğrultusunda gerekli aksiyonlar alınmaktadır.	0	0,0	0	0,0	0	0,0	3	75,0	1	25,0	17,0	4,3	0,5
Kurumda bilgi güvenliği standardı belgesine sahip olmadan önce bilgi güvenliği politikaları mevcut değildi.	0	0,0	0	0,0	2	50,0	2	50,0	0	0,0	14,0	3,5	0,6
Kurumda bilgi güvenliği standardı belgesi, belgeye sahip olmadan önceki bilgi güvenliği politikalarında bir değişikliğe sebep olmuştur.	0	0,0	0	0,0	0	0,0	3	75,0	1	25,0	17,0	4,3	0,5
Bilgi güvenliği yönetim sistemi kurulduktan sonra, öncesine göre güvenlik seviyesinde artış olmuştur.	0	0,0	0	0,0	0	0,0	4	100,0	0	0,0	16,0	4,0	0,0
Bilgi güvenliği yönetim sistemi kurulduktan sonra, öncesine göre kuruma yönelik siber saldırılarda azalma olmuştur.	0	0,0	1	25,0	1	25,0	2	50,0	0	0,0	13,0	3,3	1,0
Bilgi güvenliği yönetim sistemi kurulduktan sonra, öncesine göre kişisel ve kurumsal veri ihlallerinde azalma olmuştur.	0	0,0	0	0,0	0	0,0	3	75,0	1	25,0	17,0	4,3	0,5

Çizelge 7.2.3.'de doğal gaz sektöründe faaliyet gösteren kurumlardan BGYS biriminde görev alan personelin, BGYS çalışanları anketine verdiği yanıtların analizi yer almaktadır. Doğal gaz sektöründen ankete 4 personel katılım sağlamıştır. Katılımcı sayısının anketin diğer tüm kapsamlardan katılımcılarına oranı 5,2% olmuştur. Cevaplarda olumlu bakış açısı hakimdir. Tabloda görülebileceği üzere "Kesinlikle Katılmıyorum" seçeneğini işaretleyen katılımcı bulunmamakta, "Katılmıyorum" seçeneği ise 6 soruda işaretlenmiş bulunmaktadır. Yine 6 soru için çekimser oy kullanan personellerin olduğu görülmektedir. En düşük ortalama değeri 3,3 çıkmıştır ve 3 farklı soruda bu değere rastlanmaktadır. Aynı zamanda tüm personelin aynı seçeneği işaretlemesi ile standart sapmanın 0 değerini aldığı 4 soru bulunmaktadır. Bu 4 soruda da personel tarafından "Katılıyorum" seçeneği tercih edilmiştir.

Çizelge 7.2.4. Elektrik sektöründeki BGYS çalışanlarının cevaplarının analizi

	Kesinlikle Katılmıyorum		Katılmıyorum		Kararsızım		Katılıyorum		Kesinlikle Katılıyorum		Puan		
	f	%	f	%	f	%	f	%	f	%	Toplam	Ort.	S.Sapma
Bilgi güvenliği yönetim sistemi birimi üyeleri, sistemin kurulumu ve yürütülmesi açısından sayıca yeterlidir.	1	8,3	4	33,3	2	16,7	5	41,7	0	0,0	35,0	2,9	1,1
Bilgi güvenliği yönetim sisteminin kurulması ve yürütülmesi için kurum personeli yeterli donanıma sahiptir.	0	0,0	4	33,3	0	0,0	8	66,7	0	0,0	40,0	3,3	1,0
Bilgi güvenliği yönetim sisteminin kurulması için danışmanlık hizmeti alınmıştır.	0	0,0	0	0,0	2	16,7	9	75,0	1	8,3	47,0	3,9	0,5
Bilgi güvenliği yönetim sisteminde süreçlerin düzgün yürütülebilmesi için BGYS Birimi personeli eğitim almıştır.	0	0,0	0	0,0	1	8,3	10	83,3	1	8,3	48,0	4,0	0,4
Bilgi güvenliği yönetim sistemi bütün kurum personeli ile iş birliği içerisinde yürütülmektedir.	1	8,3	0	0,0	2	16,7	9	75,0	0	0,0	43,0	3,6	0,9
Bilgi güvenliği yönetim sistemi politikaları herkes tarafından anlaşılır düzeyde hazırlanarak kurum personeliyle birlikte tüm iç ve dış paydaşlara bildirilmektedir.	0	0,0	0	0,0	1	8,3	11	91,7	0	0,0	47,0	3,9	0,3
Bilgi güvenliği yönetim sistemi politikaları kurum bünyesindeki bütün çalışanlar tarafından benimsenmektedir.	0	0,0	2	16,7	2	16,7	8	66,7	0	0,0	42,0	3,5	0,8
Bilgi güvenliği politikası kapsamında meydana gelen değişimler, çalışanlar tarafından hali hazırda işleyen sisteme tehdit olarak algılanmamaktadır.	0	0,0	1	8,3	3	25,0	7	58,3	1	8,3	44,0	3,7	0,8
Bilgi güvenliği standartlarına sahip olmak kurumsal bilgi güvenliğini sağlamaktadır.	0	0,0	0	0,0	0	0,0	9	75,0	3	25,0	51,0	4,3	0,5
Bilgi güvenliği standartları sayesinde, kurum içi ve kurum dışındaki kritik bilgi güvenliği gereksinimleri karşılanmaktadır.	0	0,0	1	8,3	1	8,3	8	66,7	2	16,7	47,0	3,9	0,8

Çizelge 7.2.4. Elektrik sektöründeki BGYS çalışanlarının cevaplarının analizi (devam)

	Kesinlikle Katılmıyorum		Katılmıyorum		Kararsızım		Katılıyorum		Kesinlikle Katılıyorum		Puan		
	f	%	f	%	f	%	f	%	f	%	Toplam	Ort.	S.Sapma
Bilgi güvenliği sertifikasyonu sonrası süreçte, kurum personeli yeni kurallara uyum sağlamakta zorlanmamıştır.	0	0,0	2	16,7	5	41,7	5	41,7	0	0,0	39,0	3,3	0,8
BGYS Birimi, bilgi güvenliği yönetim sistemlerinin yürütülmesi sürecinde ekip dışında yer alan personelle iletişim halindedir.	0	0,0	0	0,0	2	16,7	10	83,3	0	0,0	46,0	3,8	0,4
Bilgi güvenliği yönetim sisteminin yürütülmesinde bütün birimler eşgüdümlü olarak dahil olmaktadır.	0	0,0	0	0,0	4	33,3	8	66,7	0	0,0	44,0	3,7	0,5
Bilgi güvenliği yönetim sistemi kapsamında, sürekli iyileştirmeler ve güncellemeler yapılmaktadır.	0	0,0	1	8,3	0	0,0	10	83,3	1	8,3	47,0	3,9	0,7
Bilgi güvenliği yönetim sisteminin kalitesini ölçmek adına yapılan faaliyetlerin çıktıları doğrultusunda gerekli aksiyonlar alınmaktadır.	0	0,0	0	0,0	2	16,7	10	83,3	0	0,0	46,0	3,8	0,4
Kurumda bilgi güvenliği standardı belgesine sahip olmadan önce bilgi güvenliği politikaları mevcut değildi.	0	0,0	2	16,7	2	16,7	7	58,3	1	8,3	43,0	3,6	0,9
Kurumda bilgi güvenliği standardı belgesi, belgeye sahip olmadan önceki bilgi güvenliği politikalarında bir değişikliğe sebep olmuştur.	0	0,0	1	8,3	3	25,0	7	58,3	1	8,3	44,0	3,7	0,8
Bilgi güvenliği yönetim sistemi kurulduktan sonra, öncesine göre güvenlik seviyesinde artış olmuştur.	0	0,0	0	0,0	0	0,0	10	83,3	2	16,7	50,0	4,2	0,4
Bilgi güvenliği yönetim sistemi kurulduktan sonra, öncesine göre kuruma yönelik siber saldırılarda azalma olmuştur.	0	0,0	0	0,0	4	33,3	7	58,3	1	8,3	45,0	3,8	0,6
Bilgi güvenliği yönetim sistemi kurulduktan sonra, öncesine göre kişisel ve kurumsal veri ihlallerinde azalma olmuştur.	0	0,0	0	0,0	3	25,0	7	58,3	2	16,7	47,0	3,9	0,7

Çizelge 7.2.4.'de elektrik sektöründe görev alan 12 BGYS personelinin anketteki sorulara verdiği cevapların analizi yer almaktadır. Katılımcılar, BGYS çalışanları anketinin 15,6%'sını oluşturmaktadır.

Tablo incelendiğinde en düşük ortalama değerinin 2,9 ile ilk soruda çıktığı görülmektedir. Soruda BGYS'nin kurulması ve yürütülmesi için yeterli personelin olduğunu ifade eden bir sorudur. Bu soruda olumlu ve olumsuz yanıtların sayısı eşittir. Anketin elektrik sektöründe faaliyetlerini sürdüren birden fazla kuruma gönderildiği düşünüldüğünde cevapların yoğunluğunun kurumlara göre değişiklik gösterme ihtimali bulunmaktadır. Yani bir kurumda BGYS personeli sayısının yeterli olduğu düşünülebilirken başka bir kurumda

yetersiz olduğu düşünülebilmektedir. Standart sapma ise 1,1 ile en yüksek değeri bu soru için almıştır.

En düşük standart sapma değerinin ise 0,3 olduğu görülmektedir. Bu değerin görüldüğü soru BGYS politikalarının anlaşılabilir şekilde hazırlanarak kurum personeli ile tüm iç ve dış paydaşlara bildiriliyor olmasını içermektedir. Bu husus ISO/IEC 27001 kapsamında da bir mecburiyet içermektedir. Buna paralel olarak bu soruya verilen cevap 91,7% oranı ile "Katılıyorum" seçeneği olmuştur.

Çizelge 7.2.5. Merkez teşkilattaki BGYS çalışanlarının cevaplarının analizi

	Kesinlikle Katılmıyorum		Katılmıyorum		Kararsızım		Katılıyorum		Kesinlikle Katılıyorum		Puan		
	f	%	f	%	f	%	f	%	f	%	Toplam	Ort.	S.Sapma
Bilgi güvenliği yönetim sistemi birimi üyeleri, sistemin kurulumu ve yürütülmesi açısından sayıca yeterlidir.	0	0,0	3	8,8	8	23,5	12	35,3	11	32,4	133,0	3,9	1,0
Bilgi güvenliği yönetim sisteminin kurulması ve yürütülmesi için kurum personeli yeterli donanıma sahiptir.	0	0,0	4	11,8	9	26,5	13	38,2	8	23,5	127,0	3,7	1,0
Bilgi güvenliği yönetim sisteminin kurulması için danışmanlık hizmeti alınmıştır.	0	0,0	1	2,9	16	47,1	8	23,5	9	26,5	127,0	3,7	0,9
Bilgi güvenliği yönetim sisteminde süreçlerin düzgün yürütülebilmesi için BGYS Birimi personeli eğitim almıştır.	0	0,0	2	5,9	5	14,7	13	38,2	14	41,2	141,0	4,1	0,9
Bilgi güvenliği yönetim sistemi bütün kurum personeli ile iş birliği içerisinde yürütülmektedir.	1	2,9	1	2,9	7	20,6	14	41,2	11	32,4	135,0	4,0	1,0
Bilgi güvenliği yönetim sistemi politikaları herkes tarafından anlaşılır düzeyde hazırlanarak kurum personeliyle birlikte tüm iç ve dış paydaşlara bildirilmektedir.	0	0,0	1	2,9	6	17,6	16	47,1	11	32,4	139,0	4,1	0,8
Bilgi güvenliği yönetim sistemi politikaları kurum bünyesindeki bütün çalışanlar tarafından benimsenmektedir.	0	0,0	4	11,8	10	29,4	14	41,2	6	17,6	124,0	3,6	0,9
Bilgi güvenliği politikası kapsamında meydana gelen değişimler, çalışanlar tarafından hali hazırda işleyen sisteme tehdit olarak algılanmamaktadır.	0	0,0	2	5,9	13	38,2	13	38,2	6	17,6	125,0	3,7	0,8
Bilgi güvenliği standartlarına sahip olmak kurumsal bilgi güvenliğini sağlamaktadır.	0	0,0	2	5,9	7	20,6	13	38,2	12	35,3	137,0	4,0	0,9
Bilgi güvenliği standartları sayesinde, kurum içi ve kurum dışındaki kritik bilgi güvenliği gereksinimleri karşılanmaktadır.	0	0,0	0	0,0	5	14,7	18	52,9	11	32,4	142,0	4,2	0,7

Çizelge 7.2.5. Merkez teşkilattaki BGYS çalışanlarının cevaplarının analizi (devam)

	Kesinlikle Katılmıyorum		Katılmıyorum		Kararsızım		Katılıyorum		Kesinlikle Katılıyorum		Puan		
	f	%	f	%	f	%	f	%	f	%	Toplam	Ort.	S.Sapma
Bilgi güvenliği sertifikasyonu sonrası süreçte, kurum personeli yeni kurallara uyum sağlamakta zorlanmamıştır.	0	0,0	2	5,9	9	26,5	16	47,1	7	20,6	130,0	3,8	0,8
BGYS Birimi, bilgi güvenliği yönetim sistemlerinin yürütülmesi sürecinde ekip dışında yer alan personelle iletişim halindedir.	0	0,0	4	11,8	5	14,7	18	52,9	7	20,6	130,0	3,8	0,9
Bilgi güvenliği yönetim sisteminin yürütülmesinde bütün birimler eşgüdümlü olarak dahil olmaktadır.	0	0,0	5	14,7	7	20,6	15	44,1	7	20,6	126,0	3,7	1,0
Bilgi güvenliği yönetim sistemi kapsamında, sürekli iyileştirmeler ve güncellemeler yapılmaktadır.	0	0,0	0	0,0	8	23,5	15	44,1	11	32,4	139,0	4,1	0,8
Bilgi güvenliği yönetim sisteminin kalitesini ölçmek adına yapılan faaliyetlerin çıktıları doğrultusunda gerekli aksiyonlar alınmaktadır.	0	0,0	0	0,0	8	23,5	19	55,9	7	20,6	135,0	4,0	0,7
Kurumda bilgi güvenliği standardı belgesine sahip olmadan önce bilgi güvenliği politikaları mevcut değildi.	2	5,9	1	2,9	19	55,9	10	29,4	2	5,9	111,0	3,3	0,9
Kurumda bilgi güvenliği standardı belgesi, belgeye sahip olmadan önceki bilgi güvenliği politikalarında bir değişikliğe sebep olmuştur.	0	0,0	0	0,0	11	32,4	18	52,9	5	14,7	130,0	3,8	0,7
Bilgi güvenliği yönetim sistemi kurulduktan sonra, öncesine göre güvenlik seviyesinde artış olmuştur.	1	2,9	0	0,0	5	14,7	19	55,9	9	26,5	137,0	4,0	0,8
Bilgi güvenliği yönetim sistemi kurulduktan sonra, öncesine göre kuruma yönelik siber saldırılarda azalma olmuştur.	1	2,9	0	0,0	14	41,2	9	26,5	10	29,4	129,0	3,8	1,0
Bilgi güvenliği yönetim sistemi kurulduktan sonra, öncesine göre kişisel ve kurumsal veri ihlallerinde azalma olmuştur.	0	0,0	0	0,0	9	26,5	15	44,1	10	29,4	137,0	4,0	0,8

Çizelge 7.2.5'te ETKB Merkez Teşkilatta BGYS süreçleri ile ilgili görevler üstlenen personelin ankete verdiği cevapların analizi yer almaktadır. Ankete Merkez Teşkilattan toplamda 34 kişi katılım sağlamıştır.

Bu anket, ETKB Merkez Teşkilatın BGYS birimi çalışanları ile çalıştıkları birimde BGYS sorumluluğunu üstlenen personele iletilmiştir. Diğer kapsamlarda yalnızca kurumlarının BGYS birimi çalışanlarına gönderilmiştir. Dolayısıyla tüm BGYS çalışanları anketine bakıldığında Merkez Teşkilatın katılımcı oranı 44,2% ile üstünlük sağlamaktadır.

Tablo incelendiğinde sorulara çoğunlukla olumlu yanıt verildiği görülmektedir. Bununla birlikte çekimser oy kullanan katılımcı sayısı da oldukça fazladır. Yine de analize bakıldığında bir soru hariç diğer tüm sorularda olumlu cevaplar çekimser oylardan fazla çıkmıştır. Bahsi geçen soru kurumda BGYS standardı belgelendirmesinden önce bilgi güvenliğine dair politikaların olma durumunu irdeleyen sorudur. Bu soruda 55,9% oranında "Kararsızım" seçeneği işaretlenmiştir. Bununla birlikte ortalamanın 3,3 ile en düşük değeri aldığı sorunun da bu soru olduğu görülmektedir.

Çizelge 7.2.6. Kömür sektöründeki BGYS çalışanlarının cevaplarının analizi

	Kesinlikle Katılmıyorum		Katılmıyorum		Kararsızım		Katılıyorum		Kesinlikle Katılıyorum		Puan		
	f	%	f	%	f	%	f	%	f	%	Toplam	Ort.	S.Sapma
Bilgi güvenliği yönetim sistemi birimi üyeleri, sistemin kurulumu ve yürütülmesi açısından sayıca yeterlidir.	0	0,0	4	44,4	2	22,2	3	33,3	0	0,0	26,0	2,9	0,9
Bilgi güvenliği yönetim sisteminin kurulması ve yürütülmesi için kurum personeli yeterli donanıma sahiptir.	0	0,0	4	44,4	3	33,3	2	22,2	0	0,0	25,0	2,8	0,8
Bilgi güvenliği yönetim sisteminin kurulması için danışmanlık hizmeti alınmıştır.	0	0,0	1	11,1	1	11,1	6	66,7	1	11,1	34,0	3,8	0,8
Bilgi güvenliği yönetim sisteminde süreçlerin düzgün yürütülebilmesi için BGYS Birimi personeli eğitim almıştır.	1	11,1	3	33,3	2	22,2	3	33,3	0	0,0	25,0	2,8	1,1
Bilgi güvenliği yönetim sistemi bütün kurum personeli ile iş birliği içerisinde yürütülmektedir.	0	0,0	4	44,4	2	22,2	3	33,3	0	0,0	26,0	2,9	0,9
Bilgi güvenliği yönetim sistemi politikaları herkes tarafından anlaşılır düzeyde hazırlanarak kurum personeliyle birlikte tüm iç ve dış paydaşlara bildirilmektedir.	0	0,0	1	11,1	2	22,2	6	66,7	0	0,0	32,0	3,6	0,7
Bilgi güvenliği yönetim sistemi politikaları kurum bünyesindeki bütün çalışanlar tarafından benimsenmektedir.	0	0,0	4	44,4	4	44,4	1	11,1	0	0,0	24,0	2,7	0,7
Bilgi güvenliği politikası kapsamında meydana gelen değişimler, çalışanlar tarafından hali hazırda işleyen sisteme tehdit olarak algılanmamaktadır.	0	0,0	3	33,3	3	33,3	3	33,3	0	0,0	27,0	3,0	0,9
Bilgi güvenliği standartlarına sahip olmak kurumsal bilgi güvenliğini sağlamaktadır.	0	0,0	0	0,0	1	11,1	7	77,8	1	11,1	36,0	4,0	0,5
Bilgi güvenliği standartları sayesinde, kurum içi ve kurum dışındaki kritik bilgi güvenliği gereksinimleri karşılanmaktadır.	0	0,0	0	0,0	3	33,3	6	66,7	0	0,0	33,0	3,7	0,5
Bilgi güvenliği sertifikasyonu sonrası süreçte, kurum personeli yeni kurallara uyum sağlamakta zorlanmamıştır.	0	0,0	4	44,4	1	11,1	4	44,4	0	0,0	27,0	3,0	1,0

Çizelge 7.2.6. Kömür sektöründeki BGYS çalışanlarının cevaplarının analizi (devam)

	Kesinlikle Katılmıyorum		Katılmıyorum		Kararsızım		Katılıyorum		Kesinlikle Katılıyorum		Puan		
	f	%	f	%	f	%	f	%	f	%	Toplam	Ort.	S.Sapma
BGYS Birimi, bilgi güvenliği yönetim sistemlerinin yürütülmesi sürecinde ekip dışında yer alan personelle iletişim halindedir.	0	0,0	1	11,1	1	11,1	7	77,8	0	0,0	33,0	3,7	0,7
Bilgi güvenliği yönetim sisteminin yürütülmesinde bütün birimler eşgüdümlü olarak dahil olmaktadır.	0	0,0	4	44,4	3	33,3	2	22,2	0	0,0	25,0	2,8	0,8
Bilgi güvenliği yönetim sistemi kapsamında, sürekli iyileştirmeler ve güncellemeler yapılmaktadır.	0	0,0	2	22,2	1	11,1	6	66,7	0	0,0	31,0	3,4	0,9
Bilgi güvenliği yönetim sisteminin kalitesini ölçmek adına yapılan faaliyetlerin çıktıları doğrultusunda gerekli aksiyonlar alınmaktadır.	0	0,0	0	0,0	2	22,2	7	77,8	0	0,0	34,0	3,8	0,4
Kurumda bilgi güvenliği standardı belgesine sahip olmadan önce bilgi güvenliği politikaları mevcut değildi.	0	0,0	1	11,1	6	66,7	2	22,2	0	0,0	28,0	3,1	0,6
Kurumda bilgi güvenliği standardı belgesi, belgeye sahip olmadan önceki bilgi güvenliği politikalarında bir değişikliğe sebep olmuştur.	0	0,0	0	0,0	5	55,6	3	33,3	1	11,1	32,0	3,6	0,7
Bilgi güvenliği yönetim sistemi kurulduktan sonra, öncesine göre güvenlik seviyesinde artış olmuştur.	0	0,0	0	0,0	1	11,1	6	66,7	2	22,2	37,0	4,1	0,6
Bilgi güvenliği yönetim sistemi kurulduktan sonra, öncesine göre kuruma yönelik siber saldırılarda azalma olmuştur.	0	0,0	1	11,1	3	33,3	4	44,4	1	11,1	32,0	3,6	0,9
Bilgi güvenliği yönetim sistemi kurulduktan sonra, öncesine göre kişisel ve kurumsal veri ihlallerinde azalma olmuştur.	0	0,0	0	0,0	2	22,2	6	66,7	1	11,1	35,0	3,9	0,6

Çizelge 7.2.6.'da kömür sektöründeki BGYS çalışanlarının verdiği cevapların analizine yer verilmiştir. Ankete kömür sektöründen 9 kişi katılmıştır. Katılımcı sayısı tüm BGYS çalışanları anketi katılımcılarına oranlandığında 11,7%'sini oluşturmaktadır.

Tabloya genel hatlarıyla bakıldığında birçok soruda ortalamaların düşük olduğu ve olumsuz yanıtların olduğu görülmektedir. Anketin diğer kapsamlarıyla kıyaslandığında, kömür sektöründeki cevapların ortalama değerlerinin diğerlerindeki ortalamalardan çok daha düşük olduğu görülmektedir.

En düşük ortalama değeri 2,7 çıkmıştır. Bu değerin görüldüğü soru BGYS politikalarının tüm kurum çalışanları tarafından benimsenmesinin irdelendiği sorudur. Bu soruda 44,4% oranında "Katılmıyorum", 44,4% oranında ise "Kararsızım" seçeneği işaretlenmiştir.

Bunun yanı sıra ilk iki soru da düşük ortalamaları ve dörder adet “Katılmıyorum” seçeneğini işaretleyen personelin bulunması ile dikkat çekmektedir. Bu sorularda kurum bünyesinde görev alan personelin hem sayıca hem de donanım olarak BGYS’nin kurulması ve yürütülmesi için yeterli olduğu konusu işlenmiştir. Sonuç olarak kömür sektöründe görev alan BGYS personelleri, her iki soruda da 44,4% oranıyla bu konuda olumsuz bakış açısına sahip olduklarını göstermişlerdir.

Çizelge 7.2.7. Maden sektöründeki BGYS çalışanlarının cevaplarının analizi

	Kesinlikle Katılmıyorum		Katılmıyorum		Kararsızım		Katılıyorum		Kesinlikle Katılıyorum		Puan		
	f	%	f	%	f	%	f	%	f	%	Toplam	Ort.	S.Sapma
Bilgi güvenliği yönetim sistemi birimi üyeleri, sistemin kurulumu ve yürütülmesi açısından sayıca yeterlidir.	0	0,0	1	12,5	2	25,0	4	50,0	1	12,5	29,0	3,6	0,9
Bilgi güvenliği yönetim sisteminin kurulması ve yürütülmesi için kurum personeli yeterli donanıma sahiptir.	0	0,0	1	12,5	1	12,5	6	75,0	0	0,0	29,0	3,6	0,7
Bilgi güvenliği yönetim sisteminin kurulması için danışmanlık hizmeti alınmıştır.	1	12,5	2	25,0	1	12,5	4	50,0	0	0,0	24,0	3,0	1,2
Bilgi güvenliği yönetim sisteminde süreçlerin düzgün yürütülebilmesi için BGYS Birimi personeli eğitim almıştır.	0	0,0	1	12,5	1	12,5	3	37,5	3	37,5	32,0	4,0	1,1
Bilgi güvenliği yönetim sistemi bütün kurum personeli ile iş birliği içerisinde yürütülmektedir.	0	0,0	0	0,0	1	12,5	6	75,0	1	12,5	32,0	4,0	0,5
Bilgi güvenliği yönetim sistemi politikaları herkes tarafından anlaşılır düzeyde hazırlanarak kurum personeliyle birlikte tüm iç ve dış paydaşlara bildirilmektedir.	0	0,0	0	0,0	1	12,5	5	62,5	2	25,0	33,0	4,1	0,6
Bilgi güvenliği yönetim sistemi politikaları kurum bünyesindeki bütün çalışanlar tarafından benimsenmektedir.	0	0,0	2	25,0	2	25,0	4	50,0	0	0,0	26,0	3,3	0,9
Bilgi güvenliği politikası kapsamında meydana gelen değişimler, çalışanlar tarafından hali hazırda işleyen sisteme tehdit olarak algılanmamaktadır.	0	0,0	0	0,0	2	25,0	5	62,5	1	12,5	31,0	3,9	0,6
Bilgi güvenliği standartlarına sahip olmak kurumsal bilgi güvenliğini sağlamaktadır.	0	0,0	0	0,0	0	0,0	6	75,0	2	25,0	34,0	4,3	0,5
Bilgi güvenliği standartları sayesinde, kurum içi ve kurum dışındaki kritik bilgi güvenliği gereksinimleri karşılanmaktadır.	0	0,0	0	0,0	0	0,0	7	87,5	1	12,5	33,0	4,1	0,4
Bilgi güvenliği sertifikasyonu sonrası süreçte, kurum personeli yeni kurallara uyum sağlamakta zorlanmamıştır.	0	0,0	1	12,5	2	25,0	5	62,5	0	0,0	28,0	3,5	0,8

Çizelge 7.2.7. Maden sektöründeki BGYS çalışanlarının cevaplarının analizi (devam)

	Kesinlikle Katılmıyorum		Katılmıyorum		Kararsızım		Katılıyorum		Kesinlikle Katılıyorum		Puan		
	f	%	f	%	f	%	f	%	f	%	Toplam	Ort.	S.Sapma
BGYS Birimi, bilgi güvenliği yönetim sistemlerinin yürütülmesi sürecinde ekip dışında yer alan personelle iletişim halindedir.	0	0,0	0	0,0	0	0,0	6	75,0	2	25,0	34,0	4,3	0,5
Bilgi güvenliği yönetim sisteminin yürütülmesinde bütün birimler eşgüdümlü olarak dahil olmaktadır.	0	0,0	1	12,5	1	12,5	5	62,5	1	12,5	30,0	3,7	0,9
Bilgi güvenliği yönetim sistemi kapsamında, sürekli iyileştirmeler ve güncellemeler yapılmaktadır.	0	0,0	0	0,0	1	12,5	5	62,5	2	25,0	33,0	4,1	0,6
Bilgi güvenliği yönetim sisteminin kalitesini ölçmek adına yapılan faaliyetlerin çıktıları doğrultusunda gerekli aksiyonlar alınmaktadır.	0	0,0	0	0,0	0	0,0	5	62,5	3	37,5	35,0	4,4	0,5
Kurumda bilgi güvenliği standardı belgesine sahip olmadan önce bilgi güvenliği politikaları mevcut değildi.	0	0,0	1	12,5	3	37,5	3	37,5	1	12,5	28,0	3,5	0,9
Kurumda bilgi güvenliği standardı belgesi, belgeye sahip olmadan önceki bilgi güvenliği politikalarında bir değişikliğe sebep olmuştur.	0	0,0	1	12,5	1	12,5	5	62,5	1	12,5	30,0	3,8	0,9
Bilgi güvenliği yönetim sistemi kurulduktan sonra, öncesine göre güvenlik seviyesinde artış olmuştur.	0	0,0	0	0,0	0	0,0	5	62,5	3	37,5	35,0	4,4	0,5
Bilgi güvenliği yönetim sistemi kurulduktan sonra, öncesine göre kuruma yönelik siber saldırılarda azalma olmuştur.	0	0,0	0	0,0	4	50,0	4	50,0	0	0,0	28,0	3,5	0,5
Bilgi güvenliği yönetim sistemi kurulduktan sonra, öncesine göre kişisel ve kurumsal veri ihlallerinde azalma olmuştur.	0	0,0	0	0,0	0	0,0	6	75,0	2	25,0	34,0	4,3	0,5

Maden sektöründe görev alan BGYS birimi personellerinin ankete verdikleri cevapların analizi Çizelge 7.2.7'de gösterilmektedir. Bu ankete maden sektöründe görev alan 8 BGYS personeli katılım sağlamıştır. Kapsamdaki ankete katılım sağlayan kişi sayısının genel katılıma oranı 10,4% olarak hesaplanmıştır.

Tabloda bakıldığında genel anlamda olumlu cevapların ağırlıklı olduğu görülebilmektedir. "Kesinlikle Katılmıyorum" cevabının verildiği tek bir soru mevcuttur. Bu soru kurumda BGYS kurulurken danışmanlık hizmeti alındığının sorgulandığı sorudur. Sorunun yüzdeleri incelendiğinde toplamda 37,5% olumsuz, 12,5% çekimser ve 50% olumlu cevapların mevcut olduğu görülmektedir.

Tablodan ortalama değerlerine göre olumlu cevapların fazla olduğu da açık şekilde okunmaktadır. En düşük ortalama değeri ise biraz önce bahsedilen soruda çıkmıştır.

Aynı soru için standart sapma değerinin 1,2 olduğu görülmektedir ki bu değer bu analizde hesaplanmış olan en yüksek standart sapma değeridir. En düşük standart sapma ise 0,4 değeri ile BGYS standardının kritik bilgi güvenliğinin sağladığının ifade edildiği sorudur. Bu soruda 87,5% oranında "Katılıyorum", 12,5% oranında "Kesinlikle Katılıyorum" seçeneklerin tercih edilmesiyle olumlu cevapların verildiği görülmektedir.

Çizelge 7.2.8. Nükleer sektöründeki BGYS çalışanlarının cevaplarının analizi

	Kesinlikle Katılmıyorum		Katılmıyorum		Kararsızım		Katılıyorum		Kesinlikle Katılıyorum		Puan		
	f	%	f	%	f	%	f	%	f	%	Toplam	Ort.	S.Sapma
Bilgi güvenliği yönetim sistemi birimi üyeleri, sistemin kurulumu ve yürütülmesi açısından sayıca yeterlidir.	0	0,0	0	0,0	3	60,0	2	40,0	0	0,0	17,0	3,4	0,5
Bilgi güvenliği yönetim sisteminin kurulması ve yürütülmesi için kurum personeli yeterli donanıma sahiptir.	0	0,0	1	20,0	1	20,0	3	60,0	0	0,0	17,0	3,4	0,9
Bilgi güvenliği yönetim sisteminin kurulması için danışmanlık hizmeti alınmıştır.	0	0,0	0	0,0	3	60,0	1	20,0	1	20,0	18,0	3,6	0,9
Bilgi güvenliği yönetim sisteminde süreçlerin düzgün yürütülebilmesi için BGYS Birimi personeli eğitim almıştır.	0	0,0	0	0,0	3	60,0	0	0,0	2	40,0	19,0	3,8	1,1
Bilgi güvenliği yönetim sistemi bütün kurum personeli ile iş birliği içerisinde yürütülmektedir.	1	20,0	0	0,0	1	20,0	1	20,0	2	40,0	18,0	3,6	1,7
Bilgi güvenliği yönetim sistemi politikaları herkes tarafından anlaşılır düzeyde hazırlanarak kurum personeliyle birlikte tüm iç ve dış paydaşlara bildirilmektedir.	0	0,0	1	20,0	0	0,0	3	60,0	1	20,0	19,0	3,8	1,1
Bilgi güvenliği yönetim sistemi politikaları kurum bünyesindeki bütün çalışanlar tarafından benimsenmektedir.	0	0,0	1	20,0	1	20,0	2	40,0	1	20,0	18,0	3,6	1,1
Bilgi güvenliği politikası kapsamında meydana gelen değişimler, çalışanlar tarafından hali hazırda işleyen sisteme tehdit olarak algılanmamaktadır.	0	0,0	2	40,0	1	20,0	2	40,0	0	0,0	15,0	3,0	1,0
Bilgi güvenliği standartlarına sahip olmak kurumsal bilgi güvenliğini sağlamaktadır.	0	0,0	0	0,0	0	0,0	3	60,0	2	40,0	22,0	4,4	0,5
Bilgi güvenliği standartları sayesinde, kurum içi ve kurum dışındaki kritik bilgi güvenliği gereksinimleri karşılanmaktadır.	0	0,0	0	0,0	0	0,0	3	60,0	2	40,0	22,0	4,4	0,5
Bilgi güvenliği sertifikasyonu sonrası süreçte, kurum personeli yeni kurallara uyum sağlamakta zorlanmamıştır.	0	0,0	0	0,0	4	80,0	1	20,0	0	0,0	16,0	3,2	0,4
BGYS Birimi, bilgi güvenliği yönetim sistemlerinin yürütülmesi sürecinde ekip dışında yer alan personelle iletişim halindedir.	0	0,0	1	20,0	0	0,0	3	60,0	1	20,0	19,0	3,8	1,1

Çizelge 7.2.8. Nükleer sektöründeki BGYS çalışanlarının cevaplarının analizi

	Kesinlikle Katılmıyorum		Katılmıyorum		Kararsızım		Katılıyorum		Kesinlikle Katılıyorum		Puan		
	f	%	f	%	f	%	f	%	f	%	Toplam	Ort.	S.Sapma
Bilgi güvenliği yönetim sisteminin yürütülmesinde bütün birimler eşgüdümlü olarak dahil olmaktadır.	1	20,0	0	0,0	1	20,0	1	20,0	2	40,0	18,0	3,6	1,7
Bilgi güvenliği yönetim sistemi kapsamında, sürekli iyileştirmeler ve güncellemeler yapılmaktadır.	0	0,0	0	0,0	2	40,0	2	40,0	1	20,0	19,0	3,8	0,8
Bilgi güvenliği yönetim sisteminin kalitesini ölçmek adına yapılan faaliyetlerin çıktıları doğrultusunda gerekli aksiyonlar alınmaktadır.	0	0,0	1	20,0	1	20,0	2	40,0	1	20,0	18,0	3,6	1,1
Kurumda bilgi güvenliği standardı belgesine sahip olmadan önce bilgi güvenliği politikaları mevcut değildi.	0	0,0	1	20,0	2	40,0	1	20,0	1	20,0	17,0	3,4	1,1
Kurumda bilgi güvenliği standardı belgesi, belgeye sahip olmadan önceki bilgi güvenliği politikalarında bir değişikliğe sebep olmuştur.	0	0,0	0	0,0	2	40,0	1	20,0	2	40,0	20,0	4,0	1,0
Bilgi güvenliği yönetim sistemi kurulduktan sonra, öncesine göre güvenlik seviyesinde artış olmuştur.	0	0,0	0	0,0	2	40,0	0	0,0	3	60,0	21,0	4,2	1,1
Bilgi güvenliği yönetim sistemi kurulduktan sonra, öncesine göre kuruma yönelik siber saldırılarda azalma olmuştur.	0	0,0	1	20,0	3	60,0	0	0,0	1	20,0	16,0	3,2	1,1
Bilgi güvenliği yönetim sistemi kurulduktan sonra, öncesine göre kişisel ve kurumsal veri ihlallerinde azalma olmuştur.	0	0,0	0	0,0	2	40,0	3	60,0	0	0,0	18,0	3,6	0,5

Çizelge 7.2.8.'de ankete nükleer sektörü için BGYS çalışanları tarafından verilen cevapların analizine yer verilmiştir. Ankete nükleer sektöründen 5 BGYS personeli katılım sağlamıştır. Bu kapsamdaki katılımcıların, tüm BGYS çalışanları anketine katılanlara oranı 6,5% olarak hesaplanmıştır.

Her ne kadar analizlerde çekimser oylar öne çıkmamış olsa da ortalama değerlerine bakıldığında ortalamanın genel olarak 3 civarındadır. Yani ortalama değeri hesaplanırken 1'den 5'e kadar sıralandığında "Kararsızım" seçeneğine denk gelen değere yakın sonuçlar çıkmıştır. Yine de ortalama değeri 3'ün altına düşmemiş, en düşük değer 3,0 çıkmıştır.

Ortalama değeri 3,0 olan soru BGYS politikalarındaki değişimlerin mevcut sistemi olumsuz yönde etkilemediğini ifade eden sorudur. Bu soru için cevapların oldukça dengeli olduğu görülmektedir. Bu da ortalama değerini tam olarak orta noktada göstermiştir.

Bu analiz için en yüksek standart sapma değeri 1,7'dir ve iki soruda görülmektedir. İki soru da sorulma amaçları bakımından paralellik göstermektedir. Birinde BGYS'nin tüm kurum personeli tarafından iş birliği ile yürütülmesi, diğerinde ise bütün birimlerin BGYS süreçlerine eşgüdümlü olarak dahil olması irdelenmektedir. Tablo incelendiğinde iki soruda "Kesinlikle Katılmıyorum" seçeneğinin işaretlendiği görülmektedir. Bu sorular aynı zamanda bahsi geçen, standart sapma değerlerinin en yüksek çıktığı sorulardır.

Çizelge 7.2.9. Petrol sektöründeki BGYS çalışanlarının cevaplarının analizi

	Kesinlikle Katılmıyorum		Katılmıyorum		Kararsızım		Katılıyorum		Kesinlikle Katılıyorum		Puan		
	f	%	f	%	f	%	f	%	f	%	Toplam	Ort.	S.Sapma
Bilgi güvenliği yönetim sistemi birimi üyeleri, sistemin kurulumu ve yürütülmesi açısından sayıca yeterlidir.	0	0,0	0	0,0	0	0,0	3	60,0	2	40,0	22,0	4,4	0,5
Bilgi güvenliği yönetim sisteminin kurulması ve yürütülmesi için kurum personeli yeterli donanıma sahiptir.	0	0,0	0	0,0	1	20,0	2	40,0	2	40,0	21,0	4,2	0,8
Bilgi güvenliği yönetim sisteminin kurulması için danışmanlık hizmeti alınmıştır.	0	0,0	1	20,0	1	20,0	1	20,0	2	40,0	19,0	3,8	1,3
Bilgi güvenliği yönetim sisteminde süreçlerin düzgün yürütülebilmesi için BGYS Birimi personeli eğitim almıştır.	0	0,0	0	0,0	0	0,0	3	60,0	2	40,0	22,0	4,4	0,5
Bilgi güvenliği yönetim sistemi bütün kurum personeli ile iş birliği içerisinde yürütülmektedir.	0	0,0	0	0,0	1	20,0	2	40,0	2	40,0	21,0	4,2	0,8
Bilgi güvenliği yönetim sistemi politikaları herkes tarafından anlaşılır düzeyde hazırlanarak kurum personeliyle birlikte tüm iç ve dış paydaşlara bildirilmektedir.	0	0,0	0	0,0	0	0,0	3	60,0	2	40,0	22,0	4,4	0,5
Bilgi güvenliği yönetim sistemi politikaları kurum bünyesindeki bütün çalışanlar tarafından benimsenmektedir.	0	0,0	0	0,0	1	20,0	1	20,0	3	60,0	22,0	4,4	0,9
Bilgi güvenliği politikası kapsamında meydana gelen değişimler, çalışanlar tarafından hali hazırda işleyen sisteme tehdit olarak algılanmamaktadır.	0	0,0	2	40,0	1	20,0	0	0,0	2	40,0	17,0	3,4	1,5
Bilgi güvenliği standartlarına sahip olmak kurumsal bilgi güvenliğini sağlamaktadır.	0	0,0	0	0,0	0	0,0	1	20,0	4	80,0	24,0	4,8	0,4
Bilgi güvenliği standartları sayesinde, kurum içi ve kurum dışındaki kritik bilgi güvenliği gereksinimleri karşılanmaktadır.	0	0,0	0	0,0	0	0,0	2	40,0	3	60,0	23,0	4,6	0,5
Bilgi güvenliği sertifikasyonu sonrası süreçte, kurum personeli yeni kurallara uyum sağlamakta zorlanmamıştır.	0	0,0	1	20,0	2	40,0	1	20,0	1	20,0	17,0	3,4	1,1
BGYS Birimi, bilgi güvenliği yönetim sistemlerinin yürütülmesi sürecinde ekip dışında yer alan personelle iletişim halindedir.	0	0,0	0	0,0	1	20,0	2	40,0	2	40,0	21,0	4,2	0,8

Çizelge 7.2.9. Petrol sektöründeki BGYS çalışanlarının cevaplarının analizi (devam)

	Kesinlikle Katılmıyorum		Katılmıyorum		Kararsızım		Katılıyorum		Kesinlikle Katılıyorum		Puan		
	f	%	f	%	f	%	f	%	f	%	Toplam	Ort.	S.Sapma
Bilgi güvenliği yönetim sisteminin yürütülmesinde bütün birimler eşgüdümlü olarak dahil olmaktadır.	0	0,0	1	20,0	1	20,0	1	20,0	2	40,0	19,0	3,8	1,3
Bilgi güvenliği yönetim sistemi kapsamında, sürekli iyileştirmeler ve güncellemeler yapılmaktadır.	0	0,0	0	0,0	0	0,0	3	60,0	2	40,0	22,0	4,4	0,5
Bilgi güvenliği yönetim sisteminin kalitesini ölçmek adına yapılan faaliyetlerin çıktıları doğrultusunda gerekli aksiyonlar alınmaktadır.	0	0,0	0	0,0	0	0,0	3	60,0	2	40,0	22,0	4,4	0,5
Kurumda bilgi güvenliği standardı belgesine sahip olmadan önce bilgi güvenliği politikaları mevcut değildi.	0	0,0	1	20,0	2	40,0	1	20,0	1	20,0	17,0	3,4	1,1
Kurumda bilgi güvenliği standardı belgesi, belgeye sahip olmadan önceki bilgi güvenliği politikalarında bir değişikliğe sebep olmuştur.	0	0,0	0	0,0	1	20,0	3	60,0	1	20,0	20,0	4,0	0,7
Bilgi güvenliği yönetim sistemi kurulduktan sonra, öncesine göre güvenlik seviyesinde artış olmuştur.	0	0,0	0	0,0	0	0,0	3	60,0	2	40,0	22,0	4,4	0,5
Bilgi güvenliği yönetim sistemi kurulduktan sonra, öncesine göre kuruma yönelik siber saldırılarda azalma olmuştur.	0	0,0	1	20,0	1	20,0	1	20,0	2	40,0	19,0	3,8	1,3
Bilgi güvenliği yönetim sistemi kurulduktan sonra, öncesine göre kişisel ve kurumsal veri ihlallerinde azalma olmuştur.	0	0,0	0	0,0	1	20,0	2	40,0	2	40,0	21,0	4,2	0,8

Çizelge 7.2.9.'da son kapsam olan petrol sektöründe görevli BGYS çalışanlarının verdiği cevapların analizleri bulunmaktadır. Sektörden 5 BGYS personeli ankete katılım sağlamıştır. Bu kapsamdaki katılımcıların tüm katılımcılara oranı 6,5% olarak hesaplanmıştır.

Tablo incelendiğinde diğer kapsamların çoğunda olduğu gibi burada da sorular üzerinde olumlu yanıtların hakimiyeti göze çarpmaktadır. Petrol sektöründeki BGYS personellerinden hiçbiri "Kesinlikle Katılmıyorum" seçeneğini işaretlememiştir.

En düşük ortalama olan 3,4 değeri 3 farklı soruda görülmektedir. En yüksek ortalama değeri ise 4,8 çıkmıştır. Bu değere sahip olan soruda BGYS standartlarına sahip olmanın kurumsal bilgi güvenliğini sağlamakta olduğu ifade edilmektedir. Soruya 80% oranında "Kesinlikle Katılıyorum" ve 20% oranında "Katılıyorum" cevabı verilmiştir. Bu soru aynı zamanda standart sapmanın 0,4 ile en düşük olduğu değeri aldığı sorudur.

Çizelge 7.2.10. BGYS çalışanlarının görev süresine göre olumlu ve olumsuz bakış açısının analizi

		Ne kadar süredir bu kapsamda görev almaktasınız?							
		0-5 Yıl		6-10 Yıl		10 Yıldan Fazla		Total	
		f	%	f	%	f	%	f	%
Bilgi güvenliği yönetim sistemi birimi üyeleri, sistemin kurulumu ve yürütülmesi açısından sayıca yeterlidir.	Olumlu	21	44,7	4	8,5	22	46,8	47	100,0
	Olumsuz	6	46,2	4	30,8	3	23,1	13	100,0
Bilgi güvenliği yönetim sisteminin kurulması ve yürütülmesi için kurum personeli yeterli donanıma sahiptir.	Olumlu	22	45,8	6	12,5	20	41,7	48	100,0
	Olumsuz	5	35,7	3	21,4	6	42,9	14	100,0
Bilgi güvenliği yönetim sisteminin kurulması için danışmanlık hizmeti alınmıştır.	Olumlu	19	41,3	7	15,2	20	43,5	46	100,0
	Olumsuz	3	42,9	1	14,3	3	42,9	7	100,0
Bilgi güvenliği yönetim sisteminde süreçlerin düzgün yürütülebilmesi için BGYS Birimi personeli eğitim almıştır.	Olumlu	28	48,3	8	13,8	22	37,9	58	100,0
	Olumsuz	1	14,3	4	57,1	2	28,6	7	100,0
Bilgi güvenliği yönetim sistemi bütün kurum personeli ile iş birliği içerisinde yürütülmektedir.	Olumlu	24	44,4	5	9,3	25	46,3	54	100,0
	Olumsuz	3	33,3	4	44,4	2	22,2	9	100,0
Bilgi güvenliği yönetim sistemi politikaları herkes tarafından anlaşılır düzeyde hazırlanarak kurum personeliyle birlikte tüm iç ve dış paydaşlara bildirilmektedir.	Olumlu	28	43,8	9	14,1	27	42,2	64	100,0
	Olumsuz	1	33,3	0	0,0	2	66,7	3	100,0
Bilgi güvenliği yönetim sistemi politikaları kurum bünyesindeki bütün çalışanlar tarafından benimsenmektedir.	Olumlu	19	45,2	3	7,1	20	47,6	42	100,0
	Olumsuz	3	21,4	5	35,7	6	42,9	14	100,0
Bilgi güvenliği politikası kapsamında meydana gelen değişimler, çalışanlar tarafından hali hazırda işleyen sisteme tehdit olarak algılanmamaktadır.	Olumlu	19	44,2	4	9,3	20	46,5	43	100,0
	Olumsuz	4	36,4	3	27,3	4	36,4	11	100,0
Bilgi güvenliği standartlarına sahip olmak kurumsal bilgi güvenliğini sağlamaktadır.	Olumlu	30	44,8	11	16,4	26	38,8	67	100,0
	Olumsuz	0	0,0	0	0,0	2	100,0	2	100,0
Bilgi güvenliği standartları sayesinde, kurum içi ve kurum dışındaki kritik bilgi güvenliği gereksinimleri karşılanmaktadır.	Olumlu	28	41,8	11	16,4	28	41,8	67	100,0
	Olumsuz	0	0,0	0	0,0	1	100,0	1	100,0
Bilgi güvenliği sertifikasyonu sonrası süreçte, kurum personeli yeni kurallara uyum sağlamakta zorlanmamıştır.	Olumlu	18	42,9	3	7,1	21	50,0	42	100,0
	Olumsuz	6	54,5	4	36,4	1	9,1	11	100,0
BGYS Birimi, bilgi güvenliği yönetim sistemlerinin yürütülmesi sürecinde ekip dışında yer alan personelle iletişim halindedir.	Olumlu	26	43,3	9	15,0	25	41,7	60	100,0
	Olumsuz	1	16,7	1	16,7	4	66,7	6	100,0
Bilgi güvenliği yönetim sisteminin yürütülmesinde bütün birimler eşgüdümlü olarak dahil olmaktadır.	Olumlu	21	44,7	4	8,5	22	46,8	47	100,0
	Olumsuz	7	58,3	1	8,3	4	33,3	12	100,0
Bilgi güvenliği yönetim sistemi kapsamında, sürekli iyileştirmeler ve güncellemeler yapılmaktadır.	Olumlu	27	43,5	10	16,1	25	40,3	62	100,0
	Olumsuz	1	33,3	1	33,3	1	33,3	3	100,0
Bilgi güvenliği yönetim sisteminin kalitesini ölçmek adına yapılan faaliyetlerin çıktıları doğrultusunda gerekli aksiyonlar alınmaktadır.	Olumlu	30	47,6	10	15,9	23	36,5	63	100,0
	Olumsuz	0	0,0	0	0,0	1	100,0	1	100,0

Çizelge 7.2.10. BGYS çalışanlarının görev süresine göre olumlu ve olumsuz bakış açısının analizi (devam)

		Ne kadar süredir bu kapsamda görev almaktasınız?							
		0-5 Yıl		6-10 Yıl		10 Yıldan Fazla		Total	
		f	%	f	%	f	%	f	%
Kurumda bilgi güvenliği standardı belgesine sahip olmadan önce bilgi güvenliği politikaları mevcut değildi.	Olumlu	11	34,4	7	21,9	14	43,8	32	100,0
	Olumsuz	3	33,3	1	11,1	5	55,6	9	100,0
Kurumda bilgi güvenliği standardı belgesi, belgeye sahip olmadan önceki bilgi güvenliği politikalarında bir değişikliğe sebep olmuştur.	Olumlu	21	40,4	8	15,4	23	44,2	52	100,0
	Olumsuz	1	50,0	1	50,0	0	0,0	2	100,0
Bilgi güvenliği yönetim sistemi kurulduktan sonra, öncesine göre güvenlik seviyesinde artış olmuştur.	Olumlu	30	44,1	10	14,7	28	41,2	68	100,0
	Olumsuz	0	0,0	0	0,0	1	100,0	1	100,0
Bilgi güvenliği yönetim sistemi kurulduktan sonra, öncesine göre kuruma yönelik siber saldırılarda azalma olmuştur.	Olumlu	21	50,0	3	7,1	18	42,9	42	100,0
	Olumsuz	2	40,0	1	20,0	2	40,0	5	100,0
Bilgi güvenliği yönetim sistemi kurulduktan sonra, öncesine göre kişisel ve kurumsal veri ihlallerinde azalma olmuştur.	Olumlu	27	45,0	7	11,7	26	43,3	60	100,0
	Olumsuz	0	0,0	0	0,0	0	0,0	0	0,0

Çizelge 7.2.10'da enerji sektöründeki BGYS birimi personeli ve kendi birimlerinde BGYS sorumlusu olan kişilerin "BGYS Çalışanları" anketinin "Ne kadar süredir bu kapsamda görev almaktasınız" sorusunun yanıtlarına göre, olumlu ya da olumsuz bakış açısında herhangi bir değişikliğin meydana gelip gelmediğinin analizi yer almaktadır.

"Ne kadar süredir bu kapsamda görev almaktasınız?" sorusu katılımcıyı tanımlamaya yönelik sorulmuş bir sorudur. Temel amacı görev süresiyle verilen cevapların arasında bir bağlantı olup olmadığını tespit etmektir. Örneğin; görev süresinin artmasıyla, edinilen tecrübenin BGYS'ye karşı olumlu bir bakış açısına sahip olmakta fayda sağlıyor veya daha az görev süresi için bakıldığında taze bir bakış açısıyla BGYS'nin gereklilikleri fark edilmiş ve bu doğrultuda BGYS'ye karşı olumlu bir tutum sergileniyor olabilir gibi yaklaşımların değerlendirilmesi amaçlanmıştır.

Verilen yanıtlara göre 0-5 yıl arası görev yapan personel sayısı 31, 6-10 yıl arası görev yapan personel sayısı 14 ve 10 yıldan fazla görev yapan personel sayısı 32 olduğu bilinmektedir. Tablo genel hatlarıyla incelendiğinde görev süresi ve verilen yanıtlar arasında orantısal veya herhangi bir örüntü içeren bir ilişkinin varlığından söz edilemeyeceği kanaatine varılmıştır.

7.3. Yönetim

Üst yönetimin katılım sağladığı anket cevaplarının analizleri bu bölümde yer almaktadır.

Çizelge 7.3.1. Yönetim anketi analizi genel tablo

	Kesinlikle Katılmıyorum		Katılmıyorum		Kararsızım		Katılıyorum		Kesinlikle Katılıyorum		Puan		
	f	%	f	%	f	%	f	%	f	%	Toplam	Ort.	S.Sapma
Bilgi güvenliği yönetim sistemi standartlarına sahip olmak bilgi güvenliğini korumaktadır.	0	0,0	1	2,1	1	2,1	15	31,9	30	63,8	215,0	4,6	0,7
Kritik bir güvenlik probleminde bilgi güvenliği yönetim sistemi koruma sağlamaktadır.	0	0,0	3	6,4	1	2,1	17	36,2	26	55,3	207,0	4,4	0,8
Bilgi güvenliği yönetim sistemi standartlarından uluslararası geçerliliği olan standartlara sahip olmak ulusal ve uluslararası çapta saygınlık sağlamaktadır.	0	0,0	0	0,0	3	6,4	15	31,9	29	61,7	214,0	4,6	0,6
Bilgi güvenliği yönetim sistemi standartlarının uygulanmasında yönetim önemli bir rol oynamaktadır.	1	2,1	0	0,0	1	2,1	14	29,8	31	66,0	215,0	4,6	0,7
Bilgi güvenliği yönetim sistemi politikaları kurum bünyesindeki bütün çalışanlar tarafından benimsenmektedir.	0	0,0	5	10,6	10	21,3	18	38,3	14	29,8	182,0	3,9	1,0
Bilgi güvenliği yönetimi süreçlerine, bütün birimler eşgüdümlü olarak dahil olmaktadır.	0	0,0	3	6,4	11	23,4	23	48,9	10	21,3	181,0	3,9	0,8
Bilgi güvenliği yönetimi kapsamında, sürekli iyileştirmeler ve güncellemeler yapılmaktadır.	0	0,0	0	0,0	3	6,4	25	53,2	19	40,4	204,0	4,3	0,6
Bilgi güvenliği yönetim sisteminin kalitesini ölçmek adına yapılan faaliyetlerin çıktıları doğrultusunda gerekli aksiyonlar alınmaktadır.	0	0,0	1	2,1	4	8,5	24	51,1	18	38,3	200,0	4,3	0,7
Üst yönetim bilgi güvenliği yönetim sistemini kontrol etmekte ve desteklemektedir.	0	0,0	1	2,1	2	4,3	21	44,7	23	48,9	207,0	4,4	0,7
Üst yönetimin bilgi güvenliği yönetim sistemine karşı yaklaşımı doğrultusunda sistem düzgün şekilde çalışmaktadır.	0	0,0	0	0,0	3	6,4	22	46,8	22	46,8	207,0	4,4	0,6
Üst yönetim bilgi güvenliği yönetim sistemi standardı uygulamalarından ayrıcalıklı tutulmamaktadır.	3	6,4	8	17,0	7	14,9	22	46,8	7	14,9	163,0	3,5	1,1

Çizelge 7.3.1.'de enerji sektöründe yönetici pozisyonunda görev alan katılımcıların çözdüğü yönetici anketine verilen cevapların analizi gösterilmektedir. Bu tabloda alt kırınımlara ayrılmadan sektöre yönelik genel bir analiz gerçekleştirilmiştir.

Genellikle olumlu bakış açısının hâkim olduğu sorulardan en çok olumsuz cevap alan soru, üst yönetimin BGYS uygulamalarından ayrıcalıklı tutulma durumunun sorgulandığı

sorudur. Yönetimden üst yönetime BGYS uygulamalarına karşı ayrıcalıklı tutum sergilendiğini düşünen katılımcılar bulunmaktadır. Bu soru için en yüksek 5 değerini alabilecek olan ortalama değer 3,5 çıkmıştır. Aynı zamanda bu soru standart sapma değerinin de "1,1" ile en yüksek olduğu sorudur.

Diğer sorulardan farklı olarak bu soru için her seçeneği işaretleyen katılımcı bulunduğu tablodan görülebilmektedir. Buna yakın olarak standart sapması "1" değerini alan soru BGYS politikalarının herkes tarafından benimsenip benimsenmediği sorusudur. Bu soru için de olumsuz cevap sayısı fazladır. Yöneticilerden kurum bünyesinde bulunan her personelin BGYS politikalarını benimsemediğine dair fikirlere sahip olan 5 katılımcının bulunduğu görülmektedir.

Çizelge 7.3.2. Yönetim anketi olumlu ve olumsuz yaklaşımı oranları

		f	%
Bilgi güvenliği yönetim sistemi standartlarına sahip olmak bilgi güvenliğini korumaktadır.	Olumlu	45	95,7
	Olumsuz	1	2,1
Kritik bir güvenlik probleminde bilgi güvenliği yönetim sistemi koruma sağlamaktadır.	Olumlu	43	91,5
	Olumsuz	3	6,4
Bilgi güvenliği yönetim sistemi standartlarından uluslararası geçerliliği olan standartlara sahip olmak ulusal ve uluslararası çapta saygınlık sağlamaktadır.	Olumlu	44	93,6
	Olumsuz	0	0
Bilgi güvenliği yönetim sistemi standartlarının uygulanmasında yönetim önemli bir rol oynamaktadır.	Olumlu	45	95,7
	Olumsuz	1	2,1
Bilgi güvenliği yönetim sistemi politikaları kurum bünyesindeki bütün çalışanlar tarafından benimsenmektedir.	Olumlu	32	68,1
	Olumsuz	5	10,6
Bilgi güvenliği yönetimi süreçlerine, bütün birimler eşgüdümlü olarak dahil olmaktadır.	Olumlu	33	70,2
	Olumsuz	3	6,4
Bilgi güvenliği yönetimi kapsamında, sürekli iyileştirmeler ve güncellemeler yapılmaktadır.	Olumlu	44	93,6
	Olumsuz	0	0
Bilgi güvenliği yönetim sisteminin kalitesini ölçmek adına yapılan faaliyetlerin çıktıları doğrultusunda gerekli aksiyonlar alınmaktadır.	Olumlu	42	89,4
	Olumsuz	1	2,1
Üst yönetim bilgi güvenliği yönetim sistemini kontrol etmekte ve desteklemektedir.	Olumlu	44	93,6
	Olumsuz	1	2,1
Üst yönetimin bilgi güvenliği yönetim sistemine karşı yaklaşımı doğrultusunda sistem düzgün şekilde çalışmaktadır.	Olumlu	44	93,6
	Olumsuz	0	0
Üst yönetim bilgi güvenliği yönetim sistemi standardı uygulamalarından ayrıcalıklı tutulmamaktadır.	Olumlu	29	61,7
	Olumsuz	11	23,4

Çizelge 7.3.3. Doğal gaz sektöründeki yöneticilerin cevaplarının analizi

	Kesinlikle Katılmıyorum		Katılmıyorum		Kararsızım		Katılıyorum		Kesinlikle Katılıyorum		Puan		
	f	%	f	%	f	%	f	%	f	%	Toplam	Ort.	S.Sapma
Bilgi güvenliği yönetim sistemi standartlarına sahip olmak bilgi güvenliğini korumaktadır.	0	0,0	0	0,0	0	0,0	1	25,0	3	75,0	19	4,8	0,5
Kritik bir güvenlik probleminde bilgi güvenliği yönetim sistemi koruma sağlamaktadır.	0	0,0	1	25,0	0	0,0	1	25,0	2	50,0	16	4	0,8
Bilgi güvenliği yönetim sistemi standartlarından uluslararası geçerliliği olan standartlara sahip olmak ulusal ve uluslararası çapta saygınlık sağlamaktadır.	0	0,0	0	0,0	0	0,0	1	25,0	3	75,0	19,0	4,8	0,5
Bilgi güvenliği yönetim sistemi standartlarının uygulanmasında yönetim önemli bir rol oynamaktadır.	0	0,0	0	0,0	1	25,0	1	25,0	2	50,0	17,0	4,3	1,0
Bilgi güvenliği yönetim sistemi politikaları kurum bünyesindeki bütün çalışanlar tarafından benimsenmektedir.	0	0,0	0	0,0	0	0,0	3	75,0	1	25,0	17,0	4,3	0,5
Bilgi güvenliği yönetimi süreçlerine, bütün birimler eşgüdümlü olarak dahil olmaktadır.	0	0,0	0	0,0	1	25,0	3	75,0	0	0,0	15,0	3,8	0,5
Bilgi güvenliği yönetimi kapsamında, sürekli iyileştirmeler ve güncellemeler yapılmaktadır.	0	0,0	0	0,0	0	0,0	2	50,0	2	50,0	18,0	4,5	0,6
Bilgi güvenliği yönetim sisteminin kalitesini ölçmek adına yapılan faaliyetlerin çıktıları doğrultusunda gerekli aksiyonlar alınmaktadır.	0	0,0	0	0,0	0	0,0	2	50,0	2	50,0	18,0	4,5	0,6
Üst yönetim bilgi güvenliği yönetim sistemini kontrol etmekte ve desteklemektedir.	0	0,0	0	0,0	0	0,0	2	50,0	2	50,0	18,0	4,5	0,6
Üst yönetimin bilgi güvenliği yönetim sistemine karşı yaklaşımı doğrultusunda sistem düzgün şekilde çalışmaktadır.	0	0,0	0	0,0	0	0,0	2	50,0	2	50,0	18,0	4,5	0,6
Üst yönetim bilgi güvenliği yönetim sistemi standardı uygulamalarından ayrıcalıklı tutulmamaktadır.	0	0,0	1	25,0	2	50,0	1	25,0	0	0,0	12,0	3,0	0,8

Katılımcı sayısıyla anketin %8,5'ini oluşturan doğal gaz sektöründe, yönetici pozisyonunda görev alan 4 kişinin çözdüğü yönetici anketinin sonuçlarının analizi Çizelge 7.3.3.'de gösterilmiştir. En düşük ortalama değeri; 3,0 değeri ile üst yönetimin ayrıcalıklı tutulması konusunda meydana çıkmıştır. Bu kurum içerisinde BGYS uygulamalarına yönelik irdeleme için yazılmış bir sorudur. Aynı zamanda olumsuz olarak değerlendirilen iki cevaptan biri de yine bu soruya verilmiştir. Bir diğer olumsuz cevap ise BGYS'nin kritik bir güvenlik sorununda koruma sağladığı ile ilgilidir. Bu soru ise BGYS'nin genel anlamda yapısı ile alakalı görüşlerin sorgulandığı bir sorudur.

Çizelge 7.3.4. Elektrik sektöründeki yöneticilerin cevaplarının analizi

	Kesinlikle Katılmıyorum		Katılmıyorum		Kararsızım		Katılıyorum		Kesinlikle Katılıyorum		Puan		
	f	%	f	%	f	%	f	%	f	%	Toplam	Ort.	S.Sapma
Bilgi güvenliği yönetim sistemi standartlarına sahip olmak bilgi güvenliğini korumaktadır.	0	0,0	0	0,0	0	0,0	4	44,4	5	55,6	41,0	4,6	0,5
Kritik bir güvenlik probleminde bilgi güvenliği yönetim sistemi koruma sağlamaktadır.	0	0,0	0	0,0	0	0,0	6	66,7	3	33,3	39,0	4,3	0,5
Bilgi güvenliği yönetim sistemi standartlarından uluslararası geçerliliği olan standartlara sahip olmak ulusal ve uluslararası çapta saygınlık sağlamaktadır.	0	0,0	0	0,0	1	11,1	2	22,2	6	66,7	41,0	4,6	0,7
Bilgi güvenliği yönetim sistemi standartlarının uygulanmasında yönetim önemli bir rol oynamaktadır.	0	0,0	0	0,0	0	0,0	4	44,4	5	55,6	41,0	4,6	0,5
Bilgi güvenliği yönetim sistemi politikaları kurum bünyesindeki bütün çalışanlar tarafından benimsenmektedir.	0	0,0	1	11,1	2	22,2	4	44,4	2	22,2	34,0	3,8	1,0
Bilgi güvenliği yönetimi süreçlerine, bütün birimler eşgüdümlü olarak dahil olmaktadır.	0	0,0	1	11,1	1	11,1	5	55,6	2	22,2	35,0	3,9	0,9
Bilgi güvenliği yönetimi kapsamında, sürekli iyileştirmeler ve güncellemeler yapılmaktadır.	0	0,0	0	0,0	1	11,1	6	66,7	2	22,2	37,0	4,1	0,6
Bilgi güvenliği yönetim sisteminin kalitesini ölçmek adına yapılan faaliyetlerin çıktıları doğrultusunda gerekli aksiyonlar alınmaktadır.	0	0,0	1	11,1	2	22,2	4	44,4	2	22,2	34,0	3,8	1,0
Üst yönetim bilgi güvenliği yönetim sistemini kontrol etmekte ve desteklemektedir.	0	0,0	1	11,1	0	0,0	6	66,7	2	22,2	36,0	4,0	0,9
Üst yönetimin bilgi güvenliği yönetim sistemine karşı yaklaşımı doğrultusunda sistem düzgün şekilde çalışmaktadır.	0	0,0	0	0,0	2	22,2	5	55,6	2	22,2	36,0	4,0	0,7
Üst yönetim bilgi güvenliği yönetim sistemi standardı uygulamalarından ayrıcalıklı tutulmamaktadır.	0	0,0	2	22,2	1	11,1	3	33,3	3	33,3	34,0	3,8	1,2

Yönetici anketinin 5 kişinin katılımıyla 10,6%'sını oluşturan elektrik sektöründe görev alan üst yöneticilerin verdikleri cevapların analizi Çizelge 7.3.4.'de gösterilmiştir.

Diğer alt kırınımlara göre soru sayısı olarak en fazla olumsuz yanıt bu sektörde görülmektedir. Buna rağmen 0 ve 5 arasında bir sayı alabilen ortalama değeri en az 3,8 çıkmıştır. Bu değer üç farklı soruda gözlenebilmektedir. Yine de sorulara verilen cevapların sıklıkları birbirinden farklı olduğu için standart sapma değerleri farklılık göstermektedir.

Bir diğer analiz ETKB Merkez Teşkilatta Daire Başkanlığı ve üstü makamlarda görev alan yöneticilerin verdiği cevaplar üzerinden gerçekleştirilmiş olup sonuçları Çizelge 7.3.5.'de gösterilmiştir. Katılımcı sayısı 6 kişidir ve bu anketin 12,8%'ini oluşturmaktadır.

Merkez Teşkilattan hiç olumsuz yanıt veren katılımcı olmamıştır. Özellikle iki soru için çekimser oy sayısının fazla olması 3,2 ve 3,3 gibi değerlerin çıkmasına neden olmuştur. Sorulardan bir tanesinde oy birliğine varılmasından dolayı ise, anketin diğer alt kırınımlarında rastlanmamış şekilde, standart sapma değerinin 0 çıkmasını sağlamıştır.

Çizelge 7.3.5. ETKB Merkez Teşkilatta görev alan yöneticilerin cevaplarının analizi

	Kesinlikle Katılmıyorum		Katılmıyorum		Kararsızım		Katılıyorum		Kesinlikle Katılıyorum		Puan		
	f	%	f	%	f	%	f	%	f	%	Toplam	Ort.	S.Sapma
Bilgi güvenliği yönetim sistemi standartlarına sahip olmak bilgi güvenliğini korumaktadır.	0	0,0	0	0,0	0	0,0	3	50,0	3	50,0	27,0	4,5	0,5
Kritik bir güvenlik probleminde bilgi güvenliği yönetim sistemi koruma sağlamaktadır.	0	0,0	0	0,0	0	0,0	2	33,3	4	66,7	28,0	4,7	0,5
Bilgi güvenliği yönetim sistemi standartlarından uluslararası geçerliliği olan standartlara sahip olmak ulusal ve uluslararası çapta saygınlık sağlamaktadır.	0	0,0	0	0,0	0	0,0	5	83,3	1	16,7	25,0	4,2	0,4
Bilgi güvenliği yönetim sistemi standartlarının uygulanmasında yönetim önemli bir rol oynamaktadır.	0	0,0	0	0,0	0	0,0	5	83,3	1	16,7	25,0	4,2	0,4
Bilgi güvenliği yönetim sistemi politikaları kurum bünyesindeki bütün çalışanlar tarafından benimsenmektedir.	0	0,0	0	0,0	4	66,7	2	33,3	0	0,0	20,0	3,3	0,5
Bilgi güvenliği yönetimi süreçlerine, bütün birimler eşgüdümlü olarak dahil olmaktadır.	0	0,0	0	0,0	5	83,3	1	16,7	0	0,0	19,0	3,2	0,4
Bilgi güvenliği yönetimi kapsamında, sürekli iyileştirmeler ve güncellemeler yapılmaktadır.	0	0,0	0	0,0	0	0,0	5	83,3	1	16,7	25,0	4,2	0,4
Bilgi güvenliği yönetim sisteminin kalitesini ölçmek adına yapılan faaliyetlerin çıktıları doğrultusunda gerekli aksiyonlar alınmaktadır.	0	0,0	0	0,0	0	0,0	6	100,0	0	0,0	24,0	4,0	0
Üst yönetim bilgi güvenliği yönetim sistemini kontrol etmekte ve desteklemektedir.	0	0,0	0	0,0	1	16,7	3	50,0	2	33,3	25,0	4,2	0,8
Üst yönetimin bilgi güvenliği yönetim sistemine karşı yaklaşımı doğrultusunda sistem düzgün şekilde çalışmaktadır.	0	0,0	0	0,0	1	16,7	4	66,7	1	16,7	24,0	4,0	0,6
Üst yönetim bilgi güvenliği yönetim sistemi standardı uygulamalarından ayrıcalıklı tutulmamaktadır.	0	0,0	0	0,0	2	33,3	4	66,7	0	0,0	22,0	3,7	0,5

Çizelge 7.3.6. Kömür sektöründeki yöneticilerin cevaplarının analizi

	Kesinlikle Katılmıyorum		Katılmıyorum		Kararsızım		Katılıyorum		Kesinlikle Katılıyorum		Puan		
	f	%	f	%	f	%	f	%	f	%	Toplam	Ort.	S.Sapma
Bilgi güvenliği yönetim sistemi standartlarına sahip olmak bilgi güvenliğini korumaktadır.	0	0,0	0	0,0	0	0,0	1	20,0	4	80,0	24,0	4,8	0,4
Kritik bir güvenlik probleminde bilgi güvenliği yönetim sistemi koruma sağlamaktadır.	0	0,0	0	0,0	0	0,0	1	20,0	4	80,0	24,0	4,8	0,4
Bilgi güvenliği yönetim sistemi standartlarından uluslararası geçerliliği olan standartlara sahip olmak ulusal ve uluslararası çapta saygınlık sağlamaktadır.	0	0,0	0	0,0	1	20,0	0	0,0	4	80,0	23,0	4,6	0,9
Bilgi güvenliği yönetim sistemi standartlarının uygulanmasında yönetim önemli bir rol oynamaktadır.	0	0,0	0	0,0	0	0,0	1	20,0	4	80,0	24,0	4,8	0,4
Bilgi güvenliği yönetim sistemi politikaları kurum bünyesindeki bütün çalışanlar tarafından benimsenmektedir.	0	0,0	1	20,0	0	0,0	0	0,0	4	80,0	22,0	4,4	1,3
Bilgi güvenliği yönetimi süreçlerine, bütün birimler eşgüdümlü olarak dahil olmaktadır.	0	0,0	1	20,0	0	0,0	1	20,0	3	60,0	21,0	4,2	1,3
Bilgi güvenliği yönetimi kapsamında, sürekli iyileştirmeler ve güncellemeler yapılmaktadır.	0	0,0	0	0,0	0	0,0	2	40,0	3	60,0	23,0	4,6	0,5
Bilgi güvenliği yönetim sisteminin kalitesini ölçmek adına yapılan faaliyetlerin çıktıları doğrultusunda gerekli aksiyonlar alınmaktadır.	0	0,0	0	0,0	0	0,0	2	40,0	3	60,0	23,0	4,6	0,5
Üst yönetim bilgi güvenliği yönetim sistemini kontrol etmekte ve desteklemektedir.	0	0,0	0	0,0	0	0,0	1	20,0	4	80,0	24,0	4,8	0,4
Üst yönetimin bilgi güvenliği yönetim sistemine karşı yaklaşımı doğrultusunda sistem düzgün şekilde çalışmaktadır.	0	0,0	0	0,0	0	0,0	1	20,0	4	80,0	24,0	4,8	0,4
Üst yönetim bilgi güvenliği yönetim sistemi standardı uygulamalarından ayrıcalıklı tutulmamaktadır.	2	40,0	1	20,0	0	0,0	1	20,0	1	20,0	13,0	2,6	1,8

Kömür sektöründen ankete katılan 5 yönetici bulunmaktadır ve katılımcı sayısı yönetici anketinin tüm katılımcılarının 10,6%'sını oluşturmaktadır. Kömür sektöründeki yöneticiler tarafından verilen cevapların analizi Çizelge 7.3.6'da gösterilmektedir.

Analizlerde en çok dikkat çeken son soruya verilen yanıtlardır. Bu soru üst yönetimin BGYS faaliyetlerinden ayrıcalıklı tutulup tutulmadığının irdelenebilmesi için sorulmuştur. Ağırlıklı olarak olumsuz seçeneklerin tercih edilmesi ile son sorunun ortalama puanı 2,6 çıkmıştır. Aynı soru için standart sapma değeri bu analizde en yüksek değeri olan 1,8 olduğu görülmektedir. Bu soru dışındaki sorularda ortalama oldukça yüksek değerler almıştır.

Çizelge 7.3.7. Maden sektöründeki yöneticilerin cevaplarının analizi

	Kesinlikle Katılmıyorum		Katılmıyorum		Kararsızım		Katılıyorum		Kesinlikle Katılıyorum		Puan		
	f	%	f	%	f	%	f	%	f	%	Toplam	Ort.	S.Sapma
Bilgi güvenliği yönetim sistemi standartlarına sahip olmak bilgi güvenliğini korumaktadır.	0	0,0	0	0,0	0	0,0	2	33,3	4	66,7	28,0	4,7	0,5
Kritik bir güvenlik probleminde bilgi güvenliği yönetim sistemi koruma sağlamaktadır.	0	0,0	0	0,0	0	0,0	3	50,0	3	50,0	27,0	4,5	0,5
Bilgi güvenliği yönetim sistemi standartlarından uluslararası geçerliliği olan standartlara sahip olmak ulusal ve uluslararası çapta saygınlık sağlamaktadır.	0	0,0	0	0,0	0	0,0	2	33,3	4	66,7	28,0	4,7	0,5
Bilgi güvenliği yönetim sistemi standartlarının uygulanmasında yönetim önemli bir rol oynamaktadır.	0	0,0	0	0,0	0	0,0	1	16,7	5	83,3	29,0	4,8	0,4
Bilgi güvenliği yönetim sistemi politikaları kurum bünyesindeki bütün çalışanlar tarafından benimsenmektedir.	0	0,0	0	0,0	1	16,7	2	33,3	3	50,0	26,0	4,3	0,8
Bilgi güvenliği yönetimi süreçlerine, bütün birimler eşgüdümlü olarak dahil olmaktadır.	0	0,0	0	0,0	2	33,3	2	33,3	2	33,3	24,0	4,0	0,9
Bilgi güvenliği yönetimi kapsamında, sürekli iyileştirmeler ve güncellemeler yapılmaktadır.	0	0,0	0	0,0	0	0,0	3	50,0	3	50,0	27,0	4,5	0,5
Bilgi güvenliği yönetim sisteminin kalitesini ölçmek adına yapılan faaliyetlerin çıktıları doğrultusunda gerekli aksiyonlar alınmaktadır.	0	0,0	0	0,0	0	0,0	3	50,0	3	50,0	27,0	4,5	0,5
Üst yönetim bilgi güvenliği yönetim sistemini kontrol etmekte ve desteklemektedir.	0	0,0	0	0,0	0	0,0	2	33,3	4	66,7	28,0	4,7	0,5
Üst yönetimin bilgi güvenliği yönetim sistemine karşı yaklaşımı doğrultusunda sistem düzgün şekilde çalışmaktadır.	0	0,0	0	0,0	0	0,0	3	50,0	3	50,0	27,0	4,5	0,5
Üst yönetim bilgi güvenliği yönetim sistemi standardı uygulamalarından ayrıcalıklı tutulmamaktadır.	0	0,0	1	16,7	1	16,7	3	50,0	1	16,7	22,0	3,7	1,0

Çizelge 7.3.7.'de görülebileceği üzere maden sektöründeki yöneticilerin cevapları genellikle olumlu yönde olmuştur. Çekimser oy kullanan kişi sayısı oldukça azdır. Tek olumsuz yanıt ise son soruda görülmektedir. Ankete toplamda 6 kişi katılım sağlamıştır ve katılımcı sayısı tüm anketin 12,8%'ini oluşturmaktadır.

Çizelge 7.3.8. Nükleer sektöründeki yöneticilerin cevaplarının analizi

	Kesinlikle Katılmıyorum		Katılmıyorum		Kararsızım		Katılıyorum		Kesinlikle Katılıyorum		Puan		
	f	%	f	%	f	%	f	%	f	%	Toplam	Ort.	S.Sapma
Bilgi güvenliği yönetim sistemi standartlarına sahip olmak bilgi güvenliğini korumaktadır.	0	0,0	1	8,3	0	0,0	3	25,0	8	66,7	54,0	4,5	0,9
Kritik bir güvenlik probleminde bilgi güvenliği yönetim sistemi koruma sağlamaktadır.	0	0,0	1	8,3	1	8,3	3	25,0	7	58,3	52,0	4,3	1,0
Bilgi güvenliği yönetim sistemi standartlarından uluslararası geçerliliği olan standartlara sahip olmak ulusal ve uluslararası çapta saygınlık sağlamaktadır.	0	0,0	0	0,0	1	8,3	4	33,3	7	58,3	54,0	4,5	0,7
Bilgi güvenliği yönetim sistemi standartlarının uygulanmasında yönetim önemli bir rol oynamaktadır.	0	0,0	0	0,0	0	0,0	2	16,7	10	83,3	58,0	4,8	0,4
Bilgi güvenliği yönetim sistemi politikaları kurum bünyesindeki bütün çalışanlar tarafından benimsenmektedir.	0	0,0	2	16,7	2	16,7	7	58,3	1	8,3	43,0	3,6	0,9
Bilgi güvenliği yönetimi süreçlerine, bütün birimler eşgüdümlü olarak dahil olmaktadır.	0	0,0	0	0,0	2	16,7	9	75,0	1	8,3	47,0	3,9	0,5
Bilgi güvenliği yönetimi kapsamında, sürekli iyileştirmeler ve güncellemeler yapılmaktadır.	0	0,0	0	0,0	2	16,7	5	41,7	5	41,7	51,0	4,2	0,8
Bilgi güvenliği yönetim sisteminin kalitesini ölçmek adına yapılan faaliyetlerin çıktıları doğrultusunda gerekli aksiyonlar alınmaktadır.	0	0,0	0	0,0	2	16,7	6	50,0	4	33,3	50,0	4,2	0,7
Üst yönetim bilgi güvenliği yönetim sistemini kontrol etmekte ve desteklemektedir.	0	0,0	0	0,0	1	8,3	6	50,0	5	41,7	52,0	4,3	0,7
Üst yönetimin bilgi güvenliği yönetim sistemine karşı yaklaşımı doğrultusunda sistem düzgün şekilde çalışmaktadır.	0	0,0	0	0,0	0	0,0	6	50,0	6	50,0	54,0	4,5	0,5
Üst yönetim bilgi güvenliği yönetim sistemi standardı uygulamalarından ayrıcalıklı tutulmamaktadır.	0	0,0	0	0,0	1	8,3	9	75,0	2	16,7	49,0	4,1	0,5

Nükleer alanında yönetici olan katılımcıların yanıtlarının analizleri Çizelge 7.3.8.'de gösterilmektedir. Katılımcı sayısının oranı tüm yönetici anketine katılanların 25,5%'ini oluşturmaktadır. Bu analizde en fazla olumsuz ve en yüksek çekimser yanıtlardan birine sahip olan soru BGYS uygulamalarının kurum bünyesinde çalışanlar tarafından benimsendiğini ifade eden sorudur. Ortalama değeri 3,6 ile diğer sorulara oranla en düşük değeri almıştır. Ayrıca standart sapma değeri de en yüksek ikinci değerdir.

Çizelge 7.3.9. Petrol sektöründeki yöneticilerin cevaplarının analizi

	Kesinlikle Katılmıyorum		Katılmıyorum		Kararsızım		Katılıyorum		Kesinlikle Katılıyorum		Puan		
	f	%	f	%	f	%	f	%	f	%	Toplam	Ort.	S.Sapma
Bilgi güvenliği yönetim sistemi standartlarına sahip olmak bilgi güvenliğini korumaktadır.	0	0,0	0	0,0	1	20,0	1	20,0	3	60,0	22,0	4,4	0,9
Kritik bir güvenlik probleminde bilgi güvenliği yönetim sistemi koruma sağlamaktadır.	0	0,0	1	20,0	0	0,0	1	20,0	3	60,0	21,0	4,2	1,3
Bilgi güvenliği yönetim sistemi standartlarından uluslararası geçerliliği olan standartlara sahip olmak ulusal ve uluslararası çapta saygınlık sağlamaktadır.	0	0,0	0	0,0	0	0,0	1	20,0	4	80,0	24,0	4,8	0,4
Bilgi güvenliği yönetim sistemi standartlarının uygulanmasında yönetim önemli bir rol oynamaktadır.	1	20,0	0	0,0	0	0,0	0	0,0	4	80,0	21,0	4,2	1,8
Bilgi güvenliği yönetim sistemi politikaları kurum bünyesindeki bütün çalışanlar tarafından benimsenmektedir.	0	0,0	1	20,0	1	20,0	0	0,0	3	60,0	20,0	4,0	1,4
Bilgi güvenliği yönetimi süreçlerine, bütün birimler eşgüdümlü olarak dahil olmaktadır.	0	0,0	1	20,0	0	0,0	2	40,0	2	40,0	20,0	4,0	1,2
Bilgi güvenliği yönetimi kapsamında, sürekli iyileştirmeler ve güncellemeler yapılmaktadır.	0	0,0	0	0,0	0	0,0	2	40,0	3	60,0	23,0	4,6	0,5
Bilgi güvenliği yönetim sisteminin kalitesini ölçmek adına yapılan faaliyetlerin çıktıları doğrultusunda gerekli aksiyonlar alınmaktadır.	0	0,0	0	0,0	0	0,0	1	20,0	4	80,0	24,0	4,8	0,4
Üst yönetim bilgi güvenliği yönetim sistemini kontrol etmekte ve desteklemektedir.	0	0,0	0	0,0	0	0,0	1	20,0	4	80,0	24,0	4,8	0,4
Üst yönetimin bilgi güvenliği yönetim sistemine karşı yaklaşımı doğrultusunda sistem düzgün şekilde çalışmaktadır.	0	0,0	0	0,0	0	0,0	1	20,0	4	80,0	24,0	4,8	0,4
Üst yönetim bilgi güvenliği yönetim sistemi standardı uygulamalarından ayrıcalıklı tutulmamaktadır.	1	20,0	3	60,0	0	0,0	1	20,0	0	0,0	11,0	2,2	1,1

Yönetici anketi için son kapsam petrol sektörü olarak belirlenmiş, bu kapsamda görev alan yöneticilerin verdiği cevapların analizi Çizelge 7.3.9.'da gösterilmiştir. Katılımcı sayısı tüm yönetici anketine katılanların 10,6%'sını oluşturmaktadır. Diğer kırınımların çoğunda olduğu gibi üst yönetimin BGYS uygulamalarından ayrıcalıklı tutulmaması hususunda olumsuz cevaplar görülmektedir. Bu analizde tüm sorular arasında en düşük ortalama değerine sahip olan sorudur.

Kapsam bazında diğer kırınımların analizleri ile de karşılaştırıldığında, petrol kapsamındaki analizde son sorunun aldığı ortalama değeri diğer tüm kapsamlarda aldığı değerden daha düşüktür.

Çizelge 7.3.10. İlgili kapsamdaki görev süresine göre BGYS yöneticilerinin bilgi güvenliği yönetim sistemleri konusundaki olumlu ve olumsuz düşüncelerinin dağılımı

		Ne kadar süredir bu kapsamda görev almaktasınız?							
		0-5 Yıl		6-10 Yıl		10 Yıldan Fazla		Total	
		f	%	f	%	f	%	f	%
Bilgi güvenliği yönetim sistemi standartlarına sahip olmak bilgi güvenliğini korumaktadır.	Olumlu	14	31,1	9	20,0	22	48,9	45	100,0
	Olumsuz	0	0,0	1	100,0	0	0,0	1	100,0
Kritik bir güvenlik probleminde bilgi güvenliği yönetim sistemi koruma sağlamaktadır.	Olumlu	13	30,2	9	20,9	21	48,8	43	100,0
	Olumsuz	0	0,0	1	33,3	2	66,7	3	100,0
Bilgi güvenliği yönetim sistemi standartlarından uluslararası geçerliliği olan standartlara sahip olmak ulusal ve uluslararası çapta saygınlık sağlamaktadır.	Olumlu	13	29,5	10	22,7	21	47,7	44	100,0
	Olumsuz	0	0,0	0	0,0	0	0,0	0	0,0
Bilgi güvenliği yönetim sistemi standartlarının uygulanmasında yönetim önemli bir rol oynamaktadır.	Olumlu	14	31,1	9	20,0	22	48,9	45	100,0
	Olumsuz	0	0,0	0	0,0	1	100,0	1	100,0
Bilgi güvenliği yönetim sistemi politikaları kurum bünyesindeki bütün çalışanlar tarafından benimsenmektedir.	Olumlu	8	25,0	8	25,0	16	50,0	32	100,0
	Olumsuz	2	40,0	1	20,0	2	40,0	5	100,0
Bilgi güvenliği yönetimi süreçlerine, bütün birimler eşgüdümlü olarak dahil olmaktadır.	Olumlu	10	30,3	9	27,3	14	42,4	33	100,0
	Olumsuz	0	0,0	1	33,3	2	66,7	3	100,0
Bilgi güvenliği yönetimi kapsamında, sürekli iyileştirmeler ve güncellemeler yapılmaktadır.	Olumlu	13	29,5	8	18,2	23	52,3	44	100,0
	Olumsuz	0	0,0	0	0,0	0	0,0	0	0,0
Bilgi güvenliği yönetim sisteminin kalitesini ölçmek adına yapılan faaliyetlerin çıktıları doğrultusunda gerekli aksiyonlar alınmaktadır.	Olumlu	13	31,0	8	19,0	21	50,0	42	100,0
	Olumsuz	0	0,0	1	100,0	0	0,0	1	100,0
Üst yönetim bilgi güvenliği yönetim sistemini kontrol etmekte ve desteklemektedir.	Olumlu	13	29,5	9	20,5	22	50,0	44	100,0
	Olumsuz	0	0,0	1	100,0	0	0,0	1	100,0
Üst yönetimin bilgi güvenliği yönetim sistemine karşı yaklaşımı doğrultusunda sistem düzgün şekilde çalışmaktadır.	Olumlu	14	31,8	10	22,7	20	45,5	44	100,0
	Olumsuz	0	0,0	0	0,0	0	0,0	0	0,0
Üst yönetim bilgi güvenliği yönetim sistemi standardı uygulamalarından ayrıcalıklı tutulmamaktadır.	Olumlu	7	24,1	6	20,7	16	55,2	29	100,0
	Olumsuz	4	36,4	4	36,4	3	27,3	11	100,0

Çizelge 7.3.10. toplam 47 yöneticinin katılım sağladığı anketin tanımlama sorularından üçüncüsü olan “Ne kadar süredir bu kapsamda görev almaktasınız?” sorusuna istinaden hazırlanmıştır. Tabloda ilgili kapsamdaki görev süresine göre sorulara verilen cevapların analizi görülmektedir. Süre olarak; 0-5 yıl arası görev alan katılımcı sayısının 14, 6-10 yıl arası görev alan katılımcı sayısının 10, 10 yıldan fazla süredir görev alan katılımcı sayısının ise 23 olduğu bilinmektedir. Buna göre bakıldığında katılımcıların görev süresinin BGYS’ye bakış açılarına doğrudan bir etkisi bulunmamaktadır.

8.SONUÇ

Bir kurumun en büyük sermayesi sahip olduğu bilgi varlıklarıdır. Bilgi varlıklarının hem ulusal hem de uluslararası standart, mevzuat ve kanunlarla korunması gerekmektedir. Kurumsal verilerin korunması tüm dünyada olduğu gibi, ülkemizde de hayati önem teşkil eden bir konu olarak karşımıza çıkmaktadır. Bilgi güvenliği yönetim sistemleri de bu amaca hizmet etmek üzere devreye alınmaktadır.

BGYS kapsamında gerçekleştirilen tüm faaliyetlerin kritik altyapılarda daha da önemli hale geldiği düşünüldüğünde kritik altyapı sektörleri çalışanlarının da süreçlere dahil olması yüksek önem arz etmektedir. Burada kritik altyapı çalışanlarından kastın yalnızca BGYS personeli olmadığının altının çizilmesinin de gerekli olduğu düşünülmektedir. Yani bir kurumun bünyesinde görev alan tüm çalışanların BGYS süreçlerinde rol alması beklenmektedir.

Enerji ve Tabii Kaynaklar Bakanlığı, Bakanlığa bağlı kuruluşlar ile ilgili kuruluşlar bünyesinde BGYS sistemlerinin kurulmuş olduğu ve yürütülmekte olduğu bilinmektedir. Bu çalışmada da bahsi geçen tüm kuruluşların ISO/IEC 27001 sertifikası mevcuttur. Bu kapsamda, bilgi güvenliğinin korunmasının teyidi açısından kurumlar her yıl denetim geçirmektedirler. Hem ISO/IEC 27001 denetimleri hem de Cumhurbaşkanlığı DDO Rehberi denetimlerinin geçirilmesi için yürütülen çalışmalar; kurumlar bünyesinde görev alan herkesin bilgi güvenliği hususunda bilinçli olmaları ve BGYS personellerine destek olmasıyla gerçekleşmektedir. Özellikle üst yönetimin BGYS uygulamalarına yönelik desteği ve teşviki oldukça önemlidir. Herkesin eşgüdümlü katılımı sayesinde BGYS'nin sağlıklı şekilde yürütüldüğü savunulabilir.

Literatüre bakıldığında; özellikle kurumsal anlamda BGYS'nin kurulması, yönetilmesi, düzeltici ve iyileştirici faaliyetlerin işlenmesi gibi hususlarda çalışmalara rastlanmasına karşın enerji sektöründeki bilgi güvenliği sistemlerine dair herhangi bir çalışmayla karşılaşılmamıştır. Oysaki kritik altyapı sektörlerinden biri olan enerji sektöründeki kamu kurum ve kuruluşlarında yürütülmekte olan BGYS'nin mevcut durumunun değerlendirilmesinin mühim olduğu düşünülmektedir. Bu sebepten literatürde yer alabilecek, Enerji ve Tabii Kaynaklar Bakanlığı bünyesindeki ve Bakanlığa bağlı, ilgili kuruluşlarda görevli personellerin bakış açısından BGYS'nin mevcut durumunun görülebilmesinin gerekliliği değerlendirilerek bir çalışma gerçekleştirilmesi amaçlanmıştır.

Bu amaç doğrultusunda hazırlanan çalışmada mevcut durumun analizi için personellere yönelik anketler yapılmasının doğru bir yöntem olacağı kanaatine varılmıştır. Daha önce de söz edildiği gibi BGYS tüm çalışanların el birliği ile katkıda bulunması gereken süreçlerden meydana gelmektedir. Ancak BGYS faaliyetlerinin gerçekleştirilmesinde her personelin görev ve sorumluluğu farklıdır. Dolayısıyla anket çalışmaları, personellerin gruplandırılmasının ardından gerçekleştirilmiştir. Bu gruplandırma; BGYS personelleri, yöneticiler ve geriye kalan kurum personeli olarak belirlenmiştir. Her bir grup için irdelenen hususların farklı olmasından dolayı, sorular da birbirinden farklı düzenlenmiştir. Bu sebepten bulgular da farklı kategoriler altında değerlendirilmiştir. BGYS'ye dair soruların birbirinden farklı olmasına karşın, anket katılımcısını tanımlamaya yönelik sorularda bir ortaklık söz konusudur. Tanımlama sorularında; personel anketini çözen katılımcıların hangi birimde, diğer iki anket olan yönetim anketi ile BGYS çalışanları anketi için enerji sektörünün hangi kapsamında görev aldıkları sorusu yer almaktadır. Bu kategoride yer alan bir diğer soru ise ne kadar süredir bu birimde/kapsamda görev aldıkları sorusudur. Anketlerin analizleri bu sorular üzerinden alt kırınımlara ayrılarak gerçekleştirilmiştir.

Personel anketinde katılımcıların çalıştıkları birimde ne kadar süredir görev aldıkları ile ilgili olan sorunun analizine bulguların açıklandığı bölümde yer verilmiştir ancak değerlendirilmeye alınmamıştır. Bu sorunun sorulmasındaki amaç BGYS'ye bakış açısının görev süresine göre değişip değişmediğini gözlemlemektir. Ancak personel anketinin katılımcılarının görev sürelerinin büyük çoğunluğu 0-5 yıl seçeneğinde yığılmaya sebebiyet verdiği için çıkan sonuçların doğru bir değerlendirmede kullanılamayacağı kanaatine varılmıştır.

BGYS çalışanları ve yönetim anketi için bakıldığında, görev süreleri personel anketinin sonuçlarındaki gibi bir yığılma oluşturmadığı, analiz için değerlendirilmeye yeterli veri oluşturduğu görülmüştür. Bununla beraber her iki ankette de sonuçlar incelendiğinde, diğer sorulara verilerin cevaplar ve görev süreleri arasında herhangi bir orantıya ya da örüntüye rastlanmamıştır. Bu durum bizi BGYS süreçlerine bakış açısında görev süresinin değişken bir faktör olmadığı sonucuna ulaştırmaktadır.

Anket sonuçları genel hatlarıyla incelendiğinde oldukça olumlu bir tabloyla karşılaşıldığı söylenebilmektedir. Sektörde BGYS'nin gerekliliğine, amaçlarına ve yöntemlerine karşı gerekli bilincin oluşturulduğu görülmektedir. Her anket grubu ve grupların alt kırınımları

için dikkat çeken farklı sonuçlar söz konusudur. Bu kısımda bu hususlar hakkında açıklamalara yer verilmiştir.

ETKB bünyesinde bulunan Bilgi İşlem Dairesi Başkanlığı personelinin katılımına sunulan anketin sonuçlarının analizine bulguların açıklandığı bölümde detaylı şekilde yer verilmiştir. Personel anketinin sonuçları değerlendirildiğinde; verilen olumlu cevaplar ile yüzdelik değerleri en yüksek çıkan 3 soru aşağıda, Çizelge 8.1.'de gösterilmiştir.

Çizelge 8.1. Personel anketinin en fazla olumlu yanıt alan soruları

		f	%
Kurumda, bilgi güvenliği yönetim sistemi iyi şekilde yürütülmektedir.	Olumlu	52	91,2
	Olumsuz	1	1,8
Bilgi güvenliği yönetim sistemi politikaları benimsenmekte ve desteklenmektedir.	Olumlu	51	89,4
	Olumsuz	1	1,8
Bilgi güvenliği yönetim sistemi kapsamında yapılan faaliyetler, kurumsal risk analizinin gerçekleştirilmesine katkı sağlamaktadır.	Olumlu	50	87,7
	Olumsuz	1	1,8

Çizelgeden de görülebileceği üzere bu üç sorunun olumlu cevap yüzdeleri birbirine oldukça yakındır. "Kurumda bilgi güvenliği yönetim sistemi iyi şekilde yürütülmektedir" ifadesinin fazla olumlu cevap almasında, kurum personelinin ETKB bünyesinde görev alan BGYS personelinden yana memnuniyetinin rol oynadığı yönünde yorum yapmak mümkündür. Bununla birlikte "Bilgi güvenliği yönetim sistemi politikaları benimsenmekte ve desteklenmektedir" sorusuna karşı olumlu geri dönüşler, ETKB bünyesinde görev alan her personelin BGYS'nin gerekliliklerini anlayıp benimsediği ve BGYS'ye yönelik kendini sorumlu hissettiği anlamı çıkartılabilmektedir. Bir diğer soru olan "Bilgi güvenliği yönetim sistemi kapsamında yapılan faaliyetler, kurumsal risk analizinin gerçekleştirilmesine katkı sağlamaktadır" ifadesinin yüksek derecede olumlu yanıtlanmasının ise BGYS'nin faydalarının anlaşıldığı ve yine süreçlerin herkesin katılımıyla yürütüldüğü sonucunun çıkartılmasını sağlamıştır. BGYS'nin iyi şekilde yürütülmesi ve tüm personelin bilinçli şekilde sürece katılım sağlaması bu anket için elde edilebilecek optimum sonuç olarak değerlendirilmektedir.

Personel anketinin cevapları incelendiğinde olumlu cevapların baskın olduğu görülmektedir. Bununla birlikte diğer sorulara oranla olumlu cevap yüzdesi bariz şekilde düşük olan soru ve olumsuz cevap sayısı diğer sorulara göre belirgin şekilde fazla olan soruların varlığı

görülebilmektedir. En düşük olumlu cevap yüzdesine sahip soru Çizelge 8.2.'de ve en fazla olumsuz cevaba sahip soru Çizelge 8.3.'de gösterilmiştir.

Çizelge 8.2. Personel anketinin en az olumlu yanıt alan sorusu

		f	%
Bilgi güvenliği politikası kapsamında meydana gelen değişimler, hali hazırdaki işleyişi etkilememektedir.	Olumlu	32	56,1
	Olumsuz	6	10,5

Yukarıda görülebileceği üzere en düşük olumlu cevap yüzdesine sahip olan soru "Bilgi güvenliği politikası kapsamında meydana gelen değişimler hali hazırdaki işleyişi etkilememektedir" ifadesinin bulunduğu sorudur. Bu soruda katılımcıların olumlu ya da olumsuz cevaplarının yanı sıra 33,4% oranında çekimser oy kullanıldığı hesaplanabilmektedir. BGYS kapsamında köklü değişikliklerin nadiren meydana gelmesi ya da son kullanıcıya yani BGYS çalışanları dışındaki personele yansıtılmaması sebebiyle, çekimser oy kullanan katılımcıların soru üzerinde varsayıma dayalı bir mantık yürütememesine neden olduğu düşünülmektedir. BGYS kapsamında son kullanıcıya yansıyan değişikliklerin genellikle düzeltici ve iyileştirici faaliyetler kapsamında olması gerektiği ve bu durumun işleyen sistemi etkilememesi gerektiği için 56,1% oranındaki olumlu yanıtlar makul karşılanmıştır.

Çizelge 8.3. Personel anketinin en fazla olumsuz yanıt alan sorusu

		f	%
Bilgi güvenliği yönetim sisteminin kalitesini ölçmek adına anketler yapılmaktadır.	Olumlu	37	65
	Olumsuz	9	15,8

Çizelge 8.3.'de yer alan soruda irdelenen husus BGYS çalışanları dışında yer alan personelin sistem ile alakalı fikirlerinin yeterince dikkate alınıp alınmadığı hakkındaki düşüncesinin ölçülmesidir. Bu doğrultuda personelin büyük bir çoğunluğunun olumlu yanıt verdiği görülebilmekte ancak bütün anket kendi içerisinde değerlendirildiğinde 9 katılımcının olumsuz yanıtları ile en fazla olumsuz yanıt alan soru olma özelliği taşıdığı söylenebilmektedir. BGYS'nin temel isterleri kapsamında sisteme dahil olan herkesin geri dönüşünün alınması önemli görülmektedir. Bu yüzden mevcut durumda yapılan anket sayısı ve/veya sıklığının çoğaltılmasının hem sistemin yürütülmesini sağlayan personel açısından hem kurum bünyesinde bulunan diğer personeller açısından faydalı olabileceği öngörülmektedir.

BGYS çalışanlarına yönelik anket, hem ETKB bünyesindeki BGYS birimi ve birimlerinin BGYS sorumlusu olarak görev alanlar tarafından hem de Bakanlığa bağlı ve ilgili kuruluşlarda BGYS birimlerinde görev alan personeller tarafından çözülmüştür. Anketler sonucunda elde edilen veriler bulguların açıklandığı bölümde detaylıca gösterilmiştir.

BGYS çalışanları anketinde de personel anketinde olduğu gibi tanımlamaya yönelik sorular mevcuttur. Sektörün elektrik, petrol, doğal gaz, maden, kömür, nükleer ve ETKB Merkez Teşkilat kapsamlarından hangisinde ve bu kapsamda ne kadar süredir görev alındığı sorulmuştur. İşaretlenen kapsam doğrultusunda aynı kapsamdaki kişilerin sonuçlarının kendi içerisinde değerlendirildiği kırınımlar oluşturulmuş ve bir önceki bölümde gösterilmiştir.

BGYS çalışanları anketinin sonuçları genel olarak incelendiğinde bir soru hariç her soruda olumlu cevapların ağırlıklı olduğu görülmüş, analizleri bulguların açıklandığı bölümde gerçekleştirilmiştir. Aşağıdaki tabloda yani Çizelge 8.4.'de anketin en fazla olumlu yanıt alan soruları gösterilmiştir.

Çizelge 8.4. BGYS çalışanları anketinin en fazla olumlu yanıt alan soruları

		f	%
Bilgi güvenliği yönetim sistemi kurulduktan sonra, öncesine göre güvenlik seviyesinde artış olmuştur.	Olumlu	68	88,3
	Olumsuz	1	1,3
Bilgi güvenliği standartlarına sahip olmak kurumsal bilgi güvenliğini sağlamaktadır.	Olumlu	67	87
	Olumsuz	2	2,6
Bilgi güvenliği standartları sayesinde, kurum içi ve kurum dışındaki kritik bilgi güvenliği gereksinimleri karşılanmaktadır.	Olumlu	67	87
	Olumsuz	1	1,3

Olumlu cevap yüzdesi en yüksek olan üç soruya bakıldığında BGYS çalışanları tarafından sisteme güven duyulduğu, sistemin kuruma fayda sağladığı hususunda pozitif bir bakış açısına sahip olunduğu yorumu yapılabilmektedir.

Yine ağırlıklı olarak olumlu geri dönüş alan ancak diğer sorulara nazaran daha düşük bir yüzdelik dilim olan ortalama 50% bandında seyreden yanıt oranlarına sahip sorularda, ortak bir konu olduğu göze çarpmaktadır. Bu sonuçlar, mevcut duruma bir eleştiri olarak algılanabilmektedir. Çizelge 8.5'te bahsi geçen sorulara ve cevaplarına dair analiz gösterilmiştir.

Çizelge 8.5. BGYS çalışanları anketinde kurum personeline dair ortak kanı içeren sorular

		f	%
Bilgi güvenliği politikası kapsamında meydana gelen değişimler, çalışanlar tarafından hali hazırda işleyen sisteme tehdit olarak algılanmamaktadır.	Olumlu	43	55,9
	Olumsuz	11	14,3
Bilgi güvenliği yönetim sistemi politikaları kurum bünyesindeki bütün çalışanlar tarafından benimsenmektedir.	Olumlu	42	54,6
	Olumsuz	14	18,2
Bilgi güvenliği sertifikasyonu sonrası süreçte, kurum personeli yeni kurallara uyum sağlamakta zorlanmamıştır.	Olumlu	42	54,6
	Olumsuz	11	14,3

Yukarıda yer alan tablodaki sorular, kurum bünyesinde BGYS çalışmaları haricinde görev alan personellerin BGYS uygulamalarına bakış açısının BGYS çalışanlarına nasıl yansıdığı ile ilgili analiz gerçekleştirmek amacı ile hazırlanmıştır. İlgili sorulara verilen yanıtlar incelendiğinde olumlu ve olumsuz yanıtların birbirine oldukça yakın olduğu görülmektedir. Bu doğrultuda BGYS çalışanlarından, kurum personelinin BGYS'yi tam anlamıyla benimseyemediğini düşünenlerin olduğu yorumu yapılabilmektedir. İnsanoğlunun yapısı gereğince konfor alanlarından çıkmakta zorlanması yeni kurallara, değişimlere, iyileştirme çalışmalarına karşı önyargılı olmalarına sebep olabilmektedir. Bu sorunun önüne geçilebilmesi için BGYS hakkında farkındalık eğitimlerinin sayısının ve/veya sıklığının arttırılması önerilmektedir. BGYS'nin gerekliliklerinin yeterince açık şekilde ifade edilmesi herkes tarafından benimsenmesinin anahtarı olabilmektedir.

Sorular arasından olumlu cevap yüzdesi en düşük olan soruya ise Çizelge 8.6'da yer verilmiştir. Bu soru ile ilgili dikkat çekici olan durum 50%'nin altında olumlu yanıt yüzdesinin görüldüğü tek soru olmasıdır.

Çizelge 8.6. BGYS çalışanları anketinin en az olumlu yanıt alan sorusu

		f	%
Kurumda bilgi güvenliği standardı belgesine sahip olmadan önce bilgi güvenliği politikaları mevcut değildi.	Olumlu	32	40,8
	Olumsuz	9	11,7

Yukarıdaki tabloya bakıldığında çekimser oy kullanan kişi sayısının neredeyse olumlu ve olumsuz cevap veren kişi sayısının toplamına eşit olduğu görülebilmektedir. Sorunun sorulma amacı ve yapısı değerlendirildiğinde, cevapların farklılık göstermesindeki sebebin bilgi eksiği olduğu kanaatine varılmıştır. Optimum durumda, ISO/IEC 27001 belgesine sahip olunmadan önce dahi kurumun bilgi güvenliğinin sağlanmasına yönelik politikalarının

belirlenmiş olması gerektiği düşünülmektedir. Bu soruda çekimser oy sayısı fazlalığı sorunun yorumlanması açısından bir şaibeye sebep olmaktadır.

BGYS çalışanları anketinin olumsuz yanıtları incelenirken, en fazla olumsuz yanıta sahip iki sorunun BGYS personelleri tarafından özeleştiri niteliği taşıdığı görülmektedir. Olumsuz cevap yüzdesi en yüksek olan iki soru Çizelge 8.7'da gösterilmiştir.

Çizelge 8.7. BGYS çalışanları anketinin en fazla olumsuz yanıt alan soruları

		f	%
Bilgi güvenliği yönetim sistemi birimi üyeleri, sistemin kurulumu ve yürütülmesi açısından sayıca yeterlidir.	Olumlu	47	61,1
	Olumsuz	13	16,9
Bilgi güvenliği yönetim sisteminin kurulması ve yürütülmesi için kurum personeli yeterli donanıma sahiptir.	Olumlu	48	62,4
	Olumsuz	14	18,2

Her ne kadar olumlu yanıt yüzdesi yüksek olsa da BGYS personellinin sayıca ve donanım açısından yeterli olmama ihtimali her zaman mevcuttur. Kurumların BGYS birimindeki kişi sayısının azlığı anketlerin dağıtımı sırasında fark edilmiş ve dikkat çekici bir unsur olarak not alınmıştır. Personel sayısının arttırılmasının, iş yükünün hafifletilmesi ve BGYS süreçlerinin yürütülmesinin kolaylaştırılması açısından faydalı olabileceği düşünülmektedir.

Üçüncü ve son anket olan yönetim anketi de analiz edilmiş, diğer anketler gibi bulguların açıklandığı bölümde detaylı analizlere yer verilmiştir. Yönetimin BGYS'ye bakış açısının ölçülmesinin hedeflendiği anket genel hatlarıyla incelendiğinde, olumlu cevap yüzdelerinin diğer iki anketten de daha fazla olacak şekilde karşımıza çıktığı görülmektedir. Öyle ki, 11 sorudan oluşan bu anketin 7 sorusunda 90% üzerinde, 1 sorusunda ise 89,4% oranında olumlu cevap yüzdeleriyle karşılaşılmıştır. En yüksek olumlu cevap yüzdesine sahip sorular Çizelge 8.8'de gösterilmiştir.

Çizelge 8.8. Yönetim anketinin en fazla olumlu yanıt alan soruları

		f	%
Bilgi güvenliği yönetim sistemi standartlarına sahip olmak bilgi güvenliğini korumaktadır.	Olumlu	45	95,7
	Olumsuz	1	2,1
Bilgi güvenliği yönetim sistemi standartlarının uygulanmasında yönetim önemli bir rol oynamaktadır.	Olumlu	45	95,7
	Olumsuz	1	2,1

Genel olarak yüksek yüzdeli olumlu cevaba sahip soruların tamamı ve yukarıdaki tabloda Çizelge 8.8'de ilk sırada gösterilen soru incelendiğinde yönetici pozisyonunda görev alan

kişilerin BGYS'nin temel amaç ve gerekliliklerine hâkim olduğu sonucuna ulaşılmaktadır. Bununla birlikte yukarıdaki tabloda yer verilen ikinci soruya bakıldığında, ISO/IEC 27001 standardında da açıkça belirtilen üst yönetimin BGYS'ye bakış açısının öneminin, kurumlardaki yöneticiler tarafından benimsenmiş olduğu görülmektedir.

Yönetim anketi için, en düşük olumlu cevap yüzdesi ve en yüksek olumsuz cevap yüzdesinin olduğu sorunun aynı soru olduğu görülmektedir. Soruya ve yüzdelik dilimlerine Çizelge 8.9.'da yer verilmiştir.

Çizelge 8.9. Yönetim anketinin en az olumlu ve en fazla olumsuz yanıt alan sorusu

		f	%
Üst yönetim bilgi güvenliği yönetim sistemi standardı uygulamalarından ayrıcalıklı tutulmamaktadır.	Olumlu	29	61,7
	Olumsuz	11	23,4

Bu soruda hem olumlu cevapların hem olumsuz cevapların hem de çekimser oy kullananların sayısı diğer tüm sorulara nazaran oldukça fazladır. BGYS uygulamalarının tüm kurumu kapsadığı düşünüldüğünde, üst yönetimin BGYS uygulamalarından ayrıcalıklı tutulma ihtimali oldukça kayda değer bir konudur. Kurumsal bilgi güvenliği, kişi ve pozisyon ayırt etmeden her personelin bu hususta kural ve düzenlemelere uygun davranması ile sağlanabilmektedir. Bu sebeple üst yönetime ayrıcalıklı davranılması BGYS'nin temel amaç ve prensiplerine aykırı bir tutum içerisinde bulunmak anlamına gelmektedir. Eğer var ise bu gibi beklentilerin ortadan kaldırılması için kişilerin bilgilendirilmesine yönelik gerekli açıklamalar gerçekleştirilmeli, bu gibi davranışların sergilenmesine olanak tanıyan personellerin de bu davranışlarından vazgeçmeleri hususunda gerekli çalışmalar yürütülmelidir.

Bu bölümde de bahsi geçen tüm hususlardan özetle; enerji sektöründeki BGYS uygulamalarının mevcut durumunun oldukça başarılı bir yerde seyrettiği düşünülmektedir. Enerji sektöründe BGYS kapsamında doğrudan görev almayan, yönetici pozisyonu dahil çeşitli görevlerde bulunan çalışanlar için; bilgi güvenliğine ve BGYS'ye yönelik kavramlar ile BGYS süreçleri ve uygulamalarının akılda soru bırakmayacak şekilde açıklanmasıyla, olumlu yönde görülen mevcut durumun daha da iyileştirilmesi mümkün olabilecektir. Bu doğrultuda en önemli husus farkındalık kazandırmaya yönelik çalışmalardır. Gerek mecburi olan farkındalık eğitimlerinin kapsamının genişletilmesi ve sıklığının arttırılmasıyla, gerekse sosyal mühendislik saldırıları gibi kişilerde dikkat uyandırabilecek faaliyetlerle enerji

sektörü çalışanlarında BGYS bilincinin çoğalması, bilgi güvenliğinin sürekliliğinin sekteye uğramadan korunması konusunda yarar sağlayabileceği kanaatine varılmıştır.

Diğer yandan BGYS çalışanlarının özellikle kurum personelinin BGYS süreçlerine olan katkısı konusundaki endişeleri de BGYS'nin amaç ve öneminin netleştirildikten sonra giderileceği düşünülmektedir. Ayrıca BGYS birimlerinde yeterince personelin çalışmama durumu da göz önünde bulundurulmalı ve bu konuda mümkün olan önlemler alınmalıdır. Tüm bu hususlar için üst yönetimin desteğinin çok önemli olduğu bilinmektedir. Anketler sonucunda üst yönetimin, üzerine düşen rolü yerine getirmeye açık olduğu sonucu ortaya çıkmıştır. Buradan yola çıkarak enerji sektöründe başarılı şekilde ilerleyen BGYS süreçlerinin daha da iyiye gitmesi için gerekli olan her durumun mevcut olduğu, iyileştirmelerin devamlılığının sağlanması halinde arzu edilen sonuçlara ulaşılabileceği düşünülmektedir.

Bu çalışmadan sonra, literatüre bu alanda katkı sağlayacak çalışmaların sayısının artması temenni edilmektedir. Gelecekteki çalışmalar için bazı fikir ve önerilere yer verilmek istenmektedir. Öncelikle benzer anket çalışmalarının diğer kritik altyapı sektörlerindeki kamu kurum ve kuruluşlarına yönelik gerçekleştirilmesinin kamu kurum ve kuruluşlarında BGYS farkındalığı ve etkinliğine katkı sağlayacağı düşünülmektedir. Bunun yanı sıra hem enerji sektörü için hem de diğer sektörler için gerçekleştirilecek anket çalışmalarının yöntemleri değiştirilerek farklı bakış açılarının değerlendirilebilmesi adına iyi olacağı tahmin edilmektedir. Bununla birlikte BGYS uygulamalarının ilgili personelin bakış açısından analiz edilebilmesi hususunda daha ayrıntılı sonuçlara ulaşılabilmesi açısından röportaj ve benzeri şekillerde gerçekleştirilebilecek çalışmaların etkili olacağı düşünülmektedir. Bu çalışmada uygulanan anketler için ISO/IEC 27001 standardı baz alınarak çeşitli sorular hazırlanmıştı. Her ne kadar Cumhurbaşkanlığı Dijital Dönüşüm Ofisi'nin hazırlamış olduğu Bilgi ve İletişim Güvenliği Rehberi, ISO/IEC 27001 standardı ile uyumlu olsa da kendine has bir yapısı ve çeşitli kontrolleri olduğu bilinmektedir. ETKB ve bağlı/ilgili kuruluşlarında; Rehber uyumluluğu mevcuttur ve Rehber denetimleri gerçekleştirilmektedir. Ancak ne derece etkin olduğu bilinmemektedir zira henüz Rehber'in etkinliğini ölçmeye yönelik bir çalışma yürütülmemiştir. Bununla birlikte diğer kritik altyapı sektörlerinde Rehber çalışmalarının ne durumda olduğu da meçhuldür. Her ne kadar Rehber'in uygulanma zorunluluğu olsa da uygulanmama durumuna karşın yasal bir yaptırımın düzenlenmemiş olması kurum bazında çalışmaların takibini zorlaştırmaktadır. Bu doğrultuda gelecekteki çalışmalarda kamu kurum ve kuruluşlarındaki Rehber

çalışmalarının etkinliğinin ölçülebilmesi hususu üzerinde durulmasının kurumsal anlamda ülkemizdeki bilgi güvenliğine yönelik çalışmaların mevcut durumunu şeffaf bir şekilde ortaya konulmasında faydalı olacağı düşünülmektedir.

KAYNAKLAR

1. Alkan, M. ve Canbay, C. (2004). Cenevre'den Tunus'a Dünya Bilgi Toplumu Zirvesi, *Türkiye Bilişim Derneği* 21.Ulusal Bilişim Kurultayı, pp. 291-300.
2. TDK. *Bilgi*. Türk Dil Kurumu. URL: https://sozluk.gov.tr/?q=bilgi&aranan. Son Erişim Tarihi:19.03.2024
3. Canbek, G., & Sağıroğlu, Ş. (2006). Bilgi, Bilgi Güvenliği ve Süreçleri Üzerine Bir İnceleme. *Politeknik Dergisi*, *Sayı:3, cilt:9,* 165-174.
4. Yee, C.K. ve Zolkipli, M.F. (2021). Review on confidentiality, integrity and availability in information security, *Journal of ICT in Education*, cilt 8, no. 2, 34-42.
5. Aydın, H. (2022). Yönetim Bilgi Sistemlerinde (YBS) Siber Güvenliği Önemi. *Bilgisayar Bilimleri ve Teknolojileri Dergisi*, 01-08.
6. Sakallı, B. (2017). *Kriptoloji ve Gizli Yazı Sanatı*. Medium. URL: https://medium.com/@buraksakallid/kriptoloji-ve-gizli-yazı-sanatı-dfd7b06ecd8b. Son Erişim Tarihi: 22.03.2024
7. Avaroğlu, E. (2017). Bilgi Güvenliğinin Temel Yapı Taşı: Kriptoloji. *Düşünce Dünyasında Türkiz*, 53-66.
8. EtimolojiTürkçe. *Logos*. EtmolojiTürkçe. URL: https://www.etimolojiturkce.com/kelime/logos. Son Erişim Tarihi: 19.03.2024
9. Ellison,C.(2004). *CryptographyTimeline*. CryptographyTimeline. URL: https://theworld.com/~cme /html/timeline.html. Son Erişim Tarihi: 21.03.2024
10. Tanrıverdi, E., Kurada, B., Şen, M. F., & Demirkol, K. E. (2023). Türkiye'de Afet Yönetimi Bağlamında Kritik Altyapı Kavramı. *Ankara Üniversitesi Çevrebilimleri Dergisi, 10(1)*, 1-8.
11. Ünver, M., Canbay, C., & Özkan, H. B. (2011). *Kritik Altyapıların Korunması.* Ankara: Bilgi Teknolojileri ve İletişim Kurumu.
12. National Center of Incident Readiness and Strategy For Cybersecurity (NISC). (2022). *The Cybersecurity Policy for Critical Infrastructure Prote*ction. Cybersecurity Strategic Headquarters Government of JAPAN.
13. Köksoy, F. (2023). Japonya'nın Siber Güvenlik Politikası. *Selçuk Üniversitesi Sosyal Bilimler Enstitüsü Dergisi (52)*, 249-267.
14. NIST, *NIST SP 800-82 Guide to Operational Technology Security*, 2023.
15. Dere, A. M. (2023). Endüstriyel Kontrol Sistemlerinin CVSS Tabanlı Siber Güvenlik Zafiyet Kategorisinin Tahmini İçin Bulanık Lojistik Regresyon Model Önerisi. *Doktora Tezi. Ankara, Türkiye*: Gazi Üniversitesi Fen Bilimleri Enstitüsü.
16. Hoşsavcı, G. (2008). Elektrik Enerji Sistemlerinin İzlenmesi. *Yayımlanmamış Yüksek Lisans Tezi*. Sakarya: Sakarya Üniversitesi Fen Bilimleri Enstitüsü.

17. Elektrikport. (2017). *DCS (Dağıtık Kontrol Sistemi) Nedir?* Elektrik Port. URL: https://www.elektrikport.com/teknik-kutuphane/dcs-(dagitik-kontrol-sistemi)-nedir/21167#ad-image-0. Son Erişim Tarihi: 09.02.2024

18. Yıldız, R. (2022). ISO/IEC 27001 Bilgi Güvenliği Yönetim Sistemleri Gereksinimlerinin Veri Tabanı Sistemlerinde Uygulanması. *Yüksek Lisans Tezi*. Ankara, Türkiye: Gazi Üniversitesi, Bilişim Enstitüsü.

19. Yılmaz, H. (2016). TS ISO/IEC 27001 Bilgi Güvenliği Yönetimi Standardı Kapsamında Bilgi Güvenliği Yönetim Sisteminin Kurulması ve Bilgi Güvenliği Risk Analizi. *Denetişim*, 45-59.

20. A. Marotta, F. Martinelli, S. Nanni, A. Orlando ve A. Yautsiukhin. (2017). Cyber-Insurance Survey, *Computer Science Review*, no. 24, 35-61.

21. Akay, G. (2014). Bilgi Güvenliği Yönetim Sistemleri: Bilgi Güvenliği Uygulama Mülakatları. *Yüksek Lisans Tezi*. Bilecik: Bilecik Şeyh Edebali Üniversitesi, Sosyal Bilimler Enstitüsü, İşletme Anabilim Dalı.

22. ETKB. *Misyon ve Vizyon*. T.C. Enerji ve Tabii Kaynaklar Bakanlığı. URL: https://enerji.gov.tr/kurumsal-misyon-vizyon. Son Erişim Tarihi:05.03.2024

23. MTA. *Misyon ve Vizyon*. Maden Tetkik ve Arama Genel Müdürlüğü. URL: https://www.mta.gov.tr/v3.0/kurumsal/misyon-vizyon. Son Erişim Tarihi: 07.03.2024

24. MAPEG. (2022). *Misyon ve Vizyon*. Maden ve Petrol İşleri Genel Müdürlüğü. URL: https://www.mapeg.gov.tr/Sayfa/Ozellestirilmis/misyon--vizyon. Son Erişim Tarihi: 07.03.2024

25. TEDAŞ. *Misyon ve Vizyon*. Türkiye Elektrik Dağıtım A.Ş. URL: https://www.tedas.gov.tr/tr/1/misyon-ve-vizyon/Page/63c639d6846b47cf4ea2ff5c. Son Erişim Tarihi:07.03.2024.

26. EÜAŞ. (2023). *Hakkımızda*. Elektrik Üretim A.Ş. URL: https://www.euas.gov.tr/hakkimizda. Son Erişim Tarihi: 06.03.2024

27. TEİAŞ. *Hakkımızda*. Türkiye Elektrik İletim A.Ş. URL: https://www.teias.gov.tr/hakkimizda. Son Erişim Tarihi: 07.03.2024

28. BOTAŞ. *Hakkımızda*. BOTAŞ. URL: https://www.botas.gov.tr/Sayfa/sirket-profili/472. Son Erişim Tarihi: 05.03.2024

29. TPAO. *Hakkımızda*. TPAO. URL: https://www.tpao.gov.tr/hakkimizda. Son Erişim Tarihi: 08.03.2024

30. TKİ. *Kuruluş ve Tarihçe*. Türkiye Kömür İşletmeleri Kurumu. URL: https://www.tki.gov.tr/kurulus-ve-tarihce. Son Erişim Tarihi: 07.03.2024

31. TTK. *Hakkımızda*. TTK. URL: https://www.taskomuru.gov.tr/ttk/hakkimizda/. Son Erişim Tarihi: 08.03.2024

32. ETİ MADEN. *Hakkımızda*. ETİ MADEN. URL: https://www.etimaden.gov.tr/eti-maden. Son Erişim Tarihi: 05.03.2024

33. TEMSAN. *Hakkımızda*. TEMSAN. URL: https://www.temsan.gov.tr/p/1/hakkimizda. Son Erişim Tarihi: 09.03.2024

34. TENMAK. *Hakkımızda.* TENMAK. URL: https://www.tenmak.gov.tr/kurumsal/hakkimizda.html. Son Erişim Tarihi: 09.03.2024

35. USOM. (2014). *Siber Güvenliğe İlişkin Temel Bilgiler*. Ankara: Ulusal Siber Olaylara Müdahale Merkezi, Bilgi Teknolojileri ve İletişim Kurumu Telekomünikasyon İletişim Başkanlığı.

36. Kaspersky. *Ukrayna'da BlackEnergy APT Saldırıları*. Kaspersky. URL: https://www.kaspersky.com/resource-center/threats/blackenergy. Son Erişim Tarihi:07.02.2024

37. Cerit, O. (2012). *CIH (Çernobil) Virüsü*. Microsoft. URL: https://answers.microsoft.com/tr- tr/windows/forum/all/cih-çernobil-virüsü/a1de04f7-d8eb-4d94-9e70-60c5b775affb. Son Erişim Tarihi: 10.02.2024

38. Singh, A., Choudhary, P., Singh, A. K., & Tyagi, D. K. (2021). Keylogger Detection and Prevention. *Journal of Physics: Conference Series*.

39. Çelik, S., & Çeliktaş, B. (2018). Güncel Siber Güvenlik Tehditleri: Fidye Yazılımlar. *Cyberpolitik Journal, 105-132.*

40. Biju, M., Gobal, N., & Prakash, A. (2019). Cyber Attacks And Its Dıfferent Types. *International Research Journal of Engineering and Technology (IRJET), Vol:06, Issue:03, 4849-4852.*

41. Beyaznet. (2023). *Dos ve DDos Nedir*. Beyaz Net. URL: https://www.beyaz.net/tr/guvenlik/makaleler/dos_ve_ddos_nedir.html#:~:text=Dos%20ve%20DDos%20saldırılarıyla%20amaçlanan,savaşlarda%20da%20sıklıkla%20kullanılan%20saldırılardır. Son Erişim Tarihi: 09.02.2024

42. Kaspersky. (2023). *DDosSaldırısıNedir?* Kaspersky. URL: https://www.kaspersky.com.tr/resource- center/threats/ddos-attacks#. Son Erişim Tarihi: 09.02.2024

43. Alkan, Ş. (2022,). *DOS ve DDOS Saldırı Türleri*. Medium. URL: https://servanalkan.medium.com/dos-ddos-saldırı-türleri-fe2df8834d7b. Son Erişim Tarihi: 09.02.2024

44. Uzmanposta. (2023). *SQL Injection Nedir? Nasıl Tespit Edilir? Nasıl Engellenir?* Uzman Posta. URL: https://uzmanposta.com/blog/sqlinjection/#:~:text=SQL%20injection%2C%20bir%20bilgisayar%20korsanının,olm ayan%20verilere%20erişim%20elde%20edebilir. Son Erişim Tarihi: 11.02.2024

45. Alioğlu, S. D. (2019). Siber Saldırılar ve Ülkelerin Siber Güvenlik Politikaları. *Yüksek Lisans Tezi*. İstanbul: İstanbul Bilgi Üniversitesi.

46. Kara, M. (2013). Siber Saldırılar- Siber Savaşlar Ve Etkileri. İstanbul: İstanbul Bilgi Üniversitesi, Sosyal Bilimler Enstitüsü.

47. Hoffman, D. E. (2004). Reagan Approved Plan to Sabotage Soviets. The Washington Post. URL: https://www.washingtonpost.com/archive/politics/2004/02/27/reagan-approved- plan-to-sabotage-soviets/a9184eff-47fd-402e-beb2-63970851e130/. Son Erişim Tarihi:07.02.2024

48. Tandoğan, U. (2010). Savaşa hazır mıyız? Dünya. URL: https://www.dunya.com/kose-yazisi/savasa-hazir-miyiz/7527. Son Erişim Tarihi: 07.02.2024

49. Poulsen, K. (2003). *Slammer solucanı Ohio nükleer tesis ağını çökertti*. The Register. URL: https://www.theregister.com/2003/08/20/slammer_worm_crashed_ohio_ nuke/. Son Erişim Tarihi: 15.02.2024

50. Karabacak, B. (2011). Kritik Altyapılara Yönelik Siber Tehditler ve Türkiye İçin Siber Güvenlik Önerileri. *Siber Güvenlik Çalıştayı* (s. 1- 11). Ankara: Bilgi Güvenliği Derneği.

51. Dilipraj, E. (2019). Supposed Cyber Attack On Kudankulam Nuclear Infrastructure - A Benign Reminder Of A Possıbıle Reality. *Centre for Air Power Studies*, 1-5.

52. Holloway, M. (2015). Slammer Worm and David-Besse Nuclear Plant. Stanford Edu. URL: http://large.stanford.edu/courses/2015/ph241/holloway2/. Son Erişim Tarihi: 09.02.2024

53. Hemsley, K. E., & Fisher, R. E. (2018). *History of Industrial Control System Cyber Incidents.* Idaho: Idaho National Laboratory.

54. Shull, A. (2014). Global Cybercrime: The Interplay of Politics and Law. M. Raymond, & G. Smith içinde, *Organized Chaos: Reimagining the Internet* (s. 97-103). Centre for International Governance Innovation.

55. Miller, C. (2022). *Throwback Attack: Night Dragon, one of the first attacks to target the energy industry*. Industrial Cybersecurity Pulse. URL: https://www.industrialcybersecuritypulse.com/threats-vulnerabilities/throwback-attack-night-dragon-one-of-the-first-attacks-to-target-the-energy-industry. Son Erişim Tarihi: 08.02.2024

56. Holat, O. (2021). Yeni medya ve siber savaş kavramları bağlamında Stuxnet saldırısı örneğinin incelemesi. *Abant Kültürel Araştırmalar Dergisi*, 6(11), 105-125.

57. Çelik, Ş. (2013). Stuxnet Saldırısı ve ABD'nin Siber Savaş Stratejisi: Uluslararası Hukukta Kuvvet Kullanmaktan Kaçınma İlkesi Çerçevesinde Bir Değerlendirme. *Dokuz Eylül Üniversitesi Hukuk Fakültesi Dergisi*, 137-175.

58. Khan, F. B., Asad, A., Durad, H., Mohsin, S. M., & Kazmi, S. N. (2023). Dragonfly Cyber Threats: A Case Study of Malware Attacks Targeting Power Grids. *Journal of Computing & Biomedical Informatics*, 4(02), 172-185.

59. Langill, J. T. (2014). Defending Against the Dragonfly Cyber Security Attacks. Industrial Control System Cyber Security Institute. URL: https://icscsi.org/library/Documents/Cyber_Events/Belden%20%20Defending%20Against%20the%20Dragonfly%20Cyber%20Security%20Attac ks%20v3.0.pdf. Son Erişim Tarihi: 08.02.2024

60. CheapSSL. (2017). Symantec: Hacker Grubu Dragonfly Enerji Sektörünü Hedef Aldı. CheapSSL. URL: https://cheapssl.com.tr/blog/symantec-hacker-grubu-dragonfly-enerji- sektorunu-hedef-aldi.html. Son Erişim Tarihi: 09.02.2024

61. TRT Haber. (2017). TRT Haber. Siber Tehdit Durum Raporu açıklandı. URL: https://www.trthaber.com/haber/bilim-teknoloji/siber-tehdit-durum-raporu- aciklandi-339624.html. Son Erişim Tarihi: 21.03.2024

62. Güdül, S., & Orak, B. (2023). İran'ın Siber Alandaki Faaliyetleri ve Abd ile İlişkilerine Etkisi. M. Lamba içinde, Siyaset Bilimi, *Uluslararası İlişkiler Ve Kamu Yönetimi Alanında Uluslararası Araştırmalar* (s. 151-171). Ankara: Platanus Publishing.

63. Varlık, E. (2015). ARAMCO Saldırısı. SİBERBÜLTEN. URL: https://siberbulten.com/siber- saldirilar-2/aramco-saldirisi/. Son Erişim Tarihi:16.02.2024

64. Yenienerji. (2013). Telvent, Schnneider Electric ile daha güçlü... Yenienerji. URL: https://www.yenienerji.com/roportaj/telvent-schnneider-electric-ile-daha-guclu. Son Erişim Tarihi: 09.02.2024

65. Rashid, F. (2012) Cyberwarfare. SecurityWeek. URL: https://www.securityweek.com/telvent-hit- sophisticated-cyber-attack-scada-admin-tool-compromised/. Son Erişim Tarihi: 09.02.2024

66. McCurry, J. (2014). *South Korean nuclear operator hacked amid cyber-attack fears*. The Guardian. URL: https://www.theguardian.com/world/2014/dec/22/south-korea-nuclear- power-cyber-attack-hack. Son Erişim Tarihi:13.02.2024

67. Cohen, G. (2023). *Throwback Attack: Korea Hydro and Nuclear Power highlights the vulnerability of critical systems. Industrial Cyber Security Pulse*. URL: https://www.industrialcybersecuritypulse.com/threats-vulnerabilities/throwback-attack-korea-hydro-and-nuclear-power-highlights-the-vulnerability-of-critical-systems/. Son Erişim Tarihi: 07.02.2024

68. Kaspersky. *Ukrayna'da BlackEnergy APT Saldırıları.* Kaspersky. URL: https://www.kaspersky.com/resource-center/threats/blackenergy. Son Erişim Tarihi: 07.02.2024

69. Yıldız, R. (2022). ISO/IEC 27001 Bilgi Güvenliği Yönetim Sistemleri Gereksinimlerinin Veri Tabanı Sistemlerinde Uygulanması. *Yüksek Lisans Tezi*. Ankara, Türkiye: Gazi Üniversitesi, Bilişim Enstitüsü.

70. CISA. (2021). *Cyber-Attack Against Ukrainian Critical Infrastructure*. Cybersecurity & Infrastructure Security Agency. URL: https://www.cisa.gov/news-events/ics-alerts/ir-alert-h-16-056-01. Son Erişim Tarihi: 07.02.2024

71. TDK. *Standart*. TDK. URL: https://sozluk.gov.tr/?ara=standart. Son Erişim Tarihi: 07.03.2024

72. ISO. *About ISO*. ISO. URL: https://www.iso.org/about-us.html. Son Erişim Tarihi: 22.02.2024

73. ISO. *Glossary*. ISO. URL: https://www.iso.org/glossary.html. Son Erişim Tarihi: 22.02.2024

74. ISO. *Members*. ISO. URL: https://www.iso.org/members.html URL. Son Erişim Tarihi: 22.02.2024

75. ISO. *Structure and governance*. ISO. URL: https://www.iso.org/structure.html. Son Erişim Tarihi: 22.02.2024

76. IEC. *Who we are*. IEC. URL: https://www.iec.ch/who-we-are. Son Erişim Tarihi: 22.02.2024

77. IEC. *History.* IEC. URL: https://www.iec.ch/history. Son Erişim Tarihi: 22.02.2024

78. IEC. *What we do*. IEC. URL: https://www.iec.ch/what-we-do . Son Erişim Tarihi: 22.02.2024

79. IEC. *The IEC and the Sustainable Development Goals*. IEC. URL: https://www.iec.ch/sdgs. Son Erişim Tarihi: 21.03.2024.

80. BM Türkiye. *Sürdürülebilir Kalkınma Amaçları*. BM Türkiye. URL: https://turkiye.un.org/tr/sdgs. Son Erişim Tarihi: 21.03.2024

81. IEC. *National Committees*. IEC. URL: https://www.iec.ch/national-committees. Son Erişim Tarihi: 22.02.2024

82. Yurtoğlu, N. (2018). Türk Standartları Enstitüsünün (TSE) Kuruluşu Bağlamında Türkiye'de Standardizasyon Politikaları (1923-1960). *Journal of History Studies, Volume 10 Issue 7*, 241-264.

83. ISO ve IEC. (2022). *ISO/IEC 27002 Bilgi güvenliği kontrolleri*

84. T.C. Cumburbaşkanlığı Dijital Dönüşüm Ofisi. *Hakkımızda*. T.C. Cumhurbaşkanlığı Dijital Dönüşüm Ofisi. URL: https://cbddo.gov.tr/hakkimizda/. Son Erişim Tarihi: 17.03.2024

85. DDO, (2020). *Bilgi ve İletişim Güvenliği Rehberi*, T.C. Cumhurbaşkanlığı Dijital Dönüşüm Ofisi

86. Yöntem İstatistik. (2013). *Güvenilirlik ve Geçerlilik Testleri*, Yöntem İstatistik. URL: https://www.yontemistatistik.com/post/güvenilirlik-ve-geçerlilik-testleri. Son Erişim Tarihi: 01.11.2024

87. Meral, S., & Bülbül, H. İ. (2022). Analysis of the Efficiency of the Information Security Policies of Public. *Gazi Üniversitesi Fen Bilimleri Dergisi*, 314-329.

88. ISO ve IEC. (2022). ISO/IEC 27002 *Bilgi güvenliği yönetim sistemleri-gereklilikler*

ÖZGEÇMİŞ

Kişisel Bilgiler

Soyadı, Adı : MADEN, Beyzanur
Uyruğu : T.C.

Eğitim

Derece	Eğitim Birimi	Mezuniyet Tarihi
Yüksek lisans	Gazi Üniversitesi / Adli Bilişim	Devam ediyor
Lisans	Anadolu Üniversitesi / Uluslararası İlişkiler	2022
Lisans	Başkent Üniversitesi / Elektrik Elektronik Mühendisliği	2021

İş Deneyimi

Yıl	Yer	Görev
2023-Halen	Enerji ve Tabii Kaynaklar Bakanlığı	BGYS Uzmanı
2022-2023	ELTEMTEK	Teknik Uzman Yard.

Yabancı Dil

İngilizce, İtalyanca

Yayınlar

Maden, B., & Alkan, M. (n.d.). Impact Analysis and Results of Information Security Management Systems in the Energy Sector. Turkish Journal of Mathematics and Computer Science, 16(2), 438-449. https://doi.org/10.47000/tjmcs.1537584

GAZİLİ OLMAK AYRICALIKTIR.