#### ICS03.100.70;35

**ISO 27001 BİLGİ GÜVENLİĞİ ÖZET TABLO**

#### 

**Bilgi güvenliği, siber güvenlik ve kişisel gizliliğinkorunması-Bilgigüvenliğiyönetim sistemleri - Gereklilikler**

Information security, cybersecurityandprivacyprotection—Informationsecuritymanagementsystems — Requirements

*Sécuritédel'information,cybersécuritéetprotectiondelavieprivée — Systèmes de management de la sécurité de l'information — Exigences*

Referans Numarası

ISO/IEC27001:2022(E)

©ISO/IEC2022

#### ISO/IEC27001:2022 TSISO/IEC 27001:2022

**ÇizelgeB.1—Bilgigüvenliği kontrolleri**

|  |  |  |
| --- | --- | --- |
| **5** | **Kurumsalkontroller** | |
| 5.1 | Bilgigüvenliğipolitikaları | **Kontrol**  Bilgi güvenliği politikası ve konuya özgü politikalar tanımlanmalı, yönetim tarafından onaylanmalı, yayımlanmalı, ilgili personele ve ilgili taraflara iletilmeli ve onlar tarafından onaylanmalı ve planlı aralıklarla ve önemli değişiklikler olması durumunda gözden geçirilmelidir. |
| 5.2 | Bilgigüvenliğirollerive sorumlulukları | **Kontrol**  Bilgigüvenliğirollerivesorumlulukları,kuruluşunihtiyaçlarınagöre tanımlanmalı ve dağıtılmalıdır. |
| 5.3 | Görevlerinayrılığı | **Kontrol**  Çakışangörevlerveçatışansorumlulukalanlarıbirbirindenayrılmalıdır. |
| 5.4 | Yönetimsorumlulukları | **Kontrol**  Yönetim, tüm personelinin bilgi güvenliğini kuruluşun oluşturulmuş bilgi güvenliği politikasına, konuya özgü politika ve prosedürlerine uygun olarak uygulamasını zorunlu tutmalıdır. |
| 5.5 | Yetkililerleiletişim | **Kontrol**  Kuruluş,ilgilimakamlarlailetişimkurmalıvesürdürmelidir. |
| 5.6 | Özelilgigruplarıyla iletişim | **Kontrol**  Kuruluş,özelilgigruplarıveyadiğeruzmangüvenlikforumlarıve  profesyonelderneklerleiletişimkurmalıvesürdürmelidir. |
| 5.7 | Tehditistihbaratı | **Kontrol**  Bilgi güvenliği tehditlerine ilişkin bilgiler, tehdit istihbaratı oluşturmak için toplanmalı ve analiz edilmelidir. |
| 5.8 | Projeyönetimindebilgi güvenliği | **Kontrol**  Bilgigüvenliğiprojeyönetimineentegreedilmelidir. |
| 5.9 | Bilgienvanterivediğer ilgilivarlıklar | **Kontrol**  Sahiplerdedahilolmaküzerebilgivediğerilgilivarlıklarınbirenvanteri geliştirilmeli ve sürdürülmelidir. |
| 5.10 | Bilgilerin ve diğer ilişkili varlıklarınkabuledilebilir kullanımı | **Kontrol**  Bbilgilerinvediğerilgilivarlıklarınişlenmesineyönelikkabuledilebilir kullanımkurallarıveprosedürlertanımlanmalı,dokümanteedilmelive uygulanmalıdır. |
| 5.11 | Varlıklarıniadesi | **Kontrol**  Personel ve diğer ilgili taraflar, istihdamlarının, sözleşmelerinin veya anlaşmalarının değiştirilmesi veya feshedilmesi üzerine ellerinde bulunan tüm kurumsal varlıkları uygun şekilde iade etmelidir. |

#### TSISO/IEC 27001:2022 ISO/IEC27001:2022

**ÇizelgeA.1(***devamediyor***)**

|  |  |  |
| --- | --- | --- |
| 5.12 | Bilgilerinsınıflandırılması | **Kontrol**  Bilgiler; gizlilik, bütünlük, kullanılabilirlik ve bağıntılı ilgili taraf gerekliliklerinedayalıolarakkuruluşunbilgigüvenliğiihtiyaçlarınagöre sınıflandırılmalıdır. |
| 5.13 | Bilgilerinetiketlenmesi | **Kontrol**  Bilgi etiketleme için uygun bir dizi prosedür geliştirilmeli ve kuruluş tarafından benimsenen bilgi sınıflandırma şemasına göre uygulanmalıdır. |
| 5.14 | Bilgitransferi | **Kontrol**  Kuruluş içindeki ve kuruluş ile diğer taraflar arasındaki her tip aktarım tesisi için bilgi aktarım kuralları, prosedürleri veya anlaşmaları yürürlükte olmalıdır. |
| 5.15 | Erişimkontrolu | **Kontrol**  Bilgiye ve diğer ilgili varlıklara fiziksel ve mantıksal erişimi kontrol etmeye yönelik kurallar, iş ve bilgi güvenliği gereksinimlerine dayalı olarak oluşturulmalı ve uygulanmalıdır. |
| 5.16 | Kimlikyönetimi | **Kontrol**  Kimliklerintümyaşamdöngüsüyönetilmelidir. |
| 5.17 | Kimlikdoğrulamabilgileri | **Kontrol**  Kimlik doğrulama bilgilerinin tahsisi ve yönetimi, personele kimlik doğrulama bilgilerinin uygun şekilde kullanılması konusunda tavsiye verilmesi de dahil olmak üzere bir yönetim süreci tarafından kontrol edilmelidir. |
| 5.18 | Erişimhakları | **Kontrol**  Bilgiye ve diğer ilişkili varlıklara erişim hakları, kuruluşun erişim kontrolüne ilişkinkonuya özgüpolitikasına vekurallarına uygun olarak sağlanmalı, gözden geçirilmeli, değiştirilmeli ve kaldırılmalıdır. |
| 5.19 | Tedarikçiilişkilerindebilgi güvenliği | **Kontrol**  Tedarikçinin ürün veya hizmetlerinin kullanımıyla ilgili bilgi güvenliği risklerini yönetmek için süreçler ve prosedürler tanımlanmalı ve uygulanmalıdır. |
| 5.20 | Tedarikçianlaşmalarında bilgi güvenliğinin ele alınması | **Kontrol**  İlgili bilgi güvenliği gereklilikleri, tedarikçi ilişkisinin tipine dayandırılarak her tedarikçi ile oluşturulmalı ve üzerinde anlaşmaya varılmalıdır. |
| 5.21 | Bilgiveiletişimteknolojisi (BİT) tedarik zincirinde bilgi güvenliğini yönetme | **Kontrol**  BİT ürünleri ve hizmetleri tedarik zinciri ile ilişkili bilgi güvenliği risklerini yönetmek için süreçler ve prosedürler tanımlanmalı ve uygulanmalıdır. |
| 5.22 | Tedarikçihizmetlerinin izlenmesi, gözden geçirilmesivedeğişiklik  yönetimi | **Kontrol**  Kuruluş, tedarikçi bilgi güvenliği uygulamaları ve hizmet sunumundaki değişiklikleri düzenliolarak izlemeli,gözdengeçirmeli, değerlendirmeli veyönetmelidir. |
| 5.23 | Buluthizmetlerinin kullanımı için bilgi güvenliği | **Kontrol**  Bulut hizmetlerinin edinilmesi, kullanılması, yönetimi ve bulut hizmetlerindençıkışsüreçleri,kuruluşunbilgigüvenliği gerekliliklerine uygun olarak oluşturulmalıdır. |
| 5.24 | Bilgigüvenliğiihlalolayı yönetimi planlaması ve hazırlığı | **Kontrol**  Kuruluş, bilgi güvenliği ihlal olayı yönetimi süreçlerini, rollerini ve sorumluluklarını tanımlayarak, oluşturarak ve ileterek bilgi güvenliği ihlal olaylarını yönetmeyi planlamalı ve hazırlamalıdır. |

12

#### ISO/IEC27001:2022 TSISO/IEC 27001:2022

**ÇizelgeA.1(***devamediyor***)**

|  |  |  |
| --- | --- | --- |
| 5.25 | Bilgi güvenliği ihlal olaylarını değerlendirmeve karar verme | **Kontrol**  Kuruluş, bilgi güvenliği olaylarını değerlendirmeli ve bunların bilgi güvenliği ihlal olayları olarak kategorize edilip edilmeyeceğine karar vermelidir. |
| 5.26 | Bilgi güvenliği ihlal  olaylarınayanıtverme | **Kontrol**  Bilgigüvenliğiihlalolaylarına,dokümanteedilmişprosedürlereuygun  olarakyanıtverilmelidir. |
| 5.27 | Bilgi güvenliği ihlal  olaylarındandersçıkarma | Bilgigüvenliğiihlalolaylarındaneldeedilenbilgiler,bilgigüvenliği kontrollerini güçlendirmek ve iyileştirmek amacıyla kullanılmalıdır. |
| 5.28 | Kanıttoplama | **Kontrol**  Kuruluş, bilgi güvenliği olaylarıyla ilgili kanıtların tanımlanması, toplanması, elde edilmesi ve korunması için prosedürler oluşturmalı ve uygulamalıdır. |
| 5.29 | Kesinti sırasında bilgi güvenliği | **Kontrol**  Kuruluş,kesintisırasındabilgigüvenliğiniuygunbirseviyedenasıl sürdüreceğini planlamalıdır. |
| 5.30 | İşsürekliliğiiçinBİT hazırlığı | **Kontrol**  BİThazırlığı,işsürekliliğihedefleriveBİTsürekliliğigereklilikleri temelinde planlanmalı, uygulanmalı, sürdürülmeli ve test edilmelidir. |
| 5.31 | Yasal,meşru,düzenleyici ve sözleşmeye tabi gereklilikler | **Kontrol**  Bilgi güvenliği ile ilgiliyasal, meşru, düzenleyici ve sözleşmeye tabi gereklilikler ve kuruluşun bu gereklilikleri karşılama yaklaşımı belirlenmeli, dokümante edilmeli ve güncel tutulmalıdır. |
| 5.32 | FikriMülkiyetHakları | **Kontrol**  Kuruluş,fikrimülkiyethaklarınıkorumakiçinuygunprosedürleriuygulamalıdır. |
| 5.33 | Kayıtlarınkorunması | **Kontrol**  Kayıtlarkayıpolma,tahrifedilme,sahtesiniyapma,yetkisizerişimve yetkisiz yayıma karşı korunmalıdır. |
| 5.34 | Kişiyi tespitbilgisinin (PII)gizliliğivekorunması | **Kontrol**  Kuruluş, yürürlükteki yasalara ve düzenlemelere ve sözleşme gerekliliklerine göre gizliliğin korunmasına ve PII'nin korunmasına ilişkin gereklilikleri belirlemeli ve karşılamalıdır. |
| 5.35 | Bilgigüvenliğininbağımsız gözdengeçirilmesi | **Kontrol**  İnsanlar, süreçler ve teknolojiler dahil olmak üzere Kuruluşun bilgi güvenliğini yönetme yaklaşımı ve uygulanması, planlanan aralıklarla veyaönemlideğişikliklermeydanageldiğindebağımsızolarakgözden geçirilmelidir. |
| 5.36 | Bilgigüvenliğineyönelik politikalar, kurallar ve standartlara uygunluk | **Kontrol**  Kurumunbilgigüvenliğipolitikasına,konuyaözgüpolitikalarına, kurallarınavestandartlarınauyumdüzenliolarakgözdengeçirilmelidir. |
| 5.37 | Dokümanteedilmişişletim prosedürleri | **Kontrol**  Bilgiişlemeimkanlarıiçinişletimprosedürleridokümanhaline getirilmeli ve bunlara ihtiyaç duyan personele sağlanmalıdır. |

13

#### TSISO/IEC 27001:2022 ISO/IEC27001:2022

**ÇizelgeA.1(***devamediyor***)**

|  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **6** | **Kişikontrolleri** | | | | | | | | |
| 6.1 | Tarama | **Kontrol**  Tüm personel adaylarına dair geçmiş doğrulama kontrolleri, kuruluşa katılmadanöncevesürekliolarakyürürlüktekikanunlar,yönetmeliklerveetik değerler dikkate alınarak yapılmalı ve işin gereklilikleri, erişilecek bilgilerin sınıflandırılmasına ve algılanan risklere orantılı olmalıdır. | | | | | | | |
| 6.2 | İstihdamhükümve  koşulları | **Kontrol**  İşakdisözleşmelerinde,personelinvekuruluşunbilgigüvenliğineilişkin sorumlulukları belirtilmelidir. | | | | | | | |
| 6.3 | Bilgi güvenliği farkındalığı,eğitimve öğretim | **Kontrol**  Kuruluşunpersonelivebağıntılıilgilitaraflar,işişlevleriyleilgiliolarak,uygun bilgi güvenliği farkındalığı, eğitim ve öğretim ve kuruluşun bilgi güvenliği politikası, konuya özgü politikalar ve prosedürler hakkında düzenli güncellemeleralmalıdır. | | | | | | | |
| 6.4 | Disiplinsüreci | **Kontrol**  Bilgi güvenliği politikası ihlali gerçekleştiren personele ve diğer bağıntılı ilgili taraflara karşı işlem yapılması için bir disiplin süreci resmileştirilmeli ve iletilmelidir. | | | | | | | |
| 6.5 | İstihdamınsona ermesindenveya değiştirilmesinden sonrakisorumluluklar | **Kontrol**  İstihdamın sona ermesinden veya değiştirilmesinden sonra geçerli olan bilgi güvenliği sorumlulukları ve görevleri tanımlanmalı, yürürlüğe konulmalı ve ilgili personele ve diğer ilgili taraflara iletilmelidir. | | | | | | | |
| 6.6 | Gizlilikveyaifşaetmeme anlaşmaları | **Kontrol**  Kuruluşun bilgilerin korunmasına yönelik ihtiyaçlarını yansıtan gizlilik veya ifşa etmeme anlaşmaları personel ve diğer bağıntılı taraflarca tanımlanmalı, döküman haline getirilmeli, düzenli olarak gözden geçirilmeli ve imzalanmalıdır. | | | | | | | |
| 6.7 | Uzaktançalışma | **Kontrol**  Personel, uzaktan çalışırken kuruluşun tesisleri dışında erişilen, işlenen veya depolanan bilgileri korumak için güvenlik önlemleri uygulanmalıdır. | | | | | | | |
| 6.8 | Bilgigüvenliğiolayı  raporlanması | **Kontrol**  Kuruluş, personelin gözlemlenen veya şüphelenilen bilgi güvenliği olaylarını uygun kanallar aracılığıyla zamanında raporlaması için bir mekanizma sağlamalıdır. | | | | | | | |
| **7** | **Fizikselkontroller** | | | | | | | | |
| 7.1 | Fizikselgüvenliksınırları | **Kontrol**  Bilgivediğerilişkilivarlıklarıiçerenalanlarıkorumakiçingüvenliksınırları tanımlanmalı ve kullanılmalıdır. | | | | | | | |
| 7.2 | Fizikselgiriş | **Kontrol**  Güvenlialanlar,uygungirişkontrolleriveerişimnoktalarıilekorunmalıdır. | | | | | | | |
| 7.3 | Ofislerin,odalarınve tesisleringüvenliğini sağlama | **Kontrol**  Ofisler,odalar  uygulanmalıdır. | ve | tesisler | için | fiziksel | güvenlik | tasarımlanmalı | ve |
| 7.4 | Fizikselgüvenlikizleme | **Kontrol**  Tesisleryetkisizfizikselerişimekarşısürekliolarakizlenmelidir. | | | | | | | |

14

#### ISO/IEC27001:2022 TSISO/IEC 27001:2022

**ÇizelgeA.1(***devamediyor***)**

|  |  |  |
| --- | --- | --- |
| 7.5 | Fiziksel ve çevresel tehditlerekarşıkoruma | **Kontrol**  Doğal afetler ve altyapıya yönelik diğer kasıtlı veya kasıtsız fiziksel tehditler gibi fiziksel ve çevresel tehditlere karşı koruma tasarımlanmalı ve uygulanmalıdır. |
| 7.6 | Güvenlialanlardaçalışma | **Kontrol**  Güvenlialanlardaçalışmayayönelikgüvenlikönlemleritasarımlanmalıve uygulanmalıdır. |
| 7.7 | Temizmasave temiz  ekran | **Kontrol**  Kağıtlar ve çıkarılabilir depolama ortamları için temiz masa kuralları ve bilgi işleme tesisleri için temiz ekran kuralları tanımlanmalı ve uygun şekilde uygulanmalıdır. |
| 7.8 | Ekipmankonumlandırma  vekoruma | **Kontrol**  Ekipmangüvenlibirşekildeyerleştirilmelivekorunmalıdır. |
| 7.9 | Kuruluş dışındaki varlıklarıngüvenliği | **Kontrol**  Kuruluşdışındakivarlıklarkorunmalıdır. |
| 7.10 | Depolamaortamı | **Kontrol**  Depolama ortamları, kuruluşun sınıflandırma şemasına ve taşıma gerekliliklerine uygun olarak edinme, kullanma, taşıma ve yok edilme yaşam döngüleri boyunca yönetilmelidir. |
| 7.11 | Destekleyicialtyapı hizmetleri | **Kontrol**  Bilgiişlemetesisleri,destekleyicialtyapıhizmetlerindekiarızalardankaynaklanan elektrik kesintilerinden ve diğer kesintilerden korunmalıdır. |
| 7.12 | Kablogüvenliği | **Kontrol**  Güç, veri veya destekleyici bilgi servislerini taşıyan kablolar, dinleme, girişim veya hasara karşı korunmalıdır. |
| 7.13 | Ekipmanbakımı | **Kontrol**  Bilgininkullanılabilirliğini(yararlanabilirliğini),bütünlüğünüvegizliliğini sağlamak için ekipman bakımı doğru bir şekilde yapılmalıdır. |
| 7.14 | Ekipmanın güvenli bir şekildeyokedilmesiveya tekrar kullanılması | **Kontrol**  Depolama ortamı içeren ekipman öğeleri, tüm hassas verilerin ve lisanslı yazılımların yok edilmeden veya tekrar kullanılmadan önce kaldırıldığından veya güvenli bir şekilde üzerine yazıldığından emin olmak için doğrulanmalıdır. |
| **8** | **Teknolojikkontroller** | |
| 8.1 | Kullanıcıuçnokta cihazları | **Kontrol**  Kullanıcıuçnoktacihazlarındadepolanan,bunlartarafındanişlenenveya bunlar aracılığıyla erişilen bilgiler korunmalıdır. |
| 8.2 | Ayrıcalıklıerişimhakları | **Kontrol**  Ayrıcalıklıerişimhaklarınıntahsisivekullanımısınırlandırılmalıve yönetilmelidir. |
| 8.3 | Bilgierişimkısıtlaması | **Kontrol**  Bilgilerevediğerilgilivarlıklaraerişim,erişimkontrolükonusundaoluşturulmuş konuya özgü politikaya uygun olarak kısıtlanmalıdır. |
| 8.4 | Kaynakkodunaerişim | **Kontrol**  Kaynakkoduna,geliştirmearaçlarınaveyazılımkütüphanelerineokumave  yazmaerişimiuygunşekildeyönetilmelidir. |

15

#### TSISO/IEC 27001:2022 ISO/IEC27001:2022

**ÇizelgeA.1(***devamediyor***)**

|  |  |  |
| --- | --- | --- |
| 8.5 | Güvenlikimlikdoğrulama | **Kontrol**  Güvenli kimlik doğrulama teknolojileri ve prosedürleri, bilgi erişim kısıtlamalarına ve erişim kontrolüne ilişkin konuya özgü politikaya dayalı olarak uygulanmalıdır. |
| 8.6 | Kapasiteyönetimi | **Kontrol**  Kaynakların kullanımı izlenmeli ve mevcut ve beklenen kapasite gereklilikleri doğrultusunda ayarlanmalıdır. |
| 8.7 | Kötüamaçlıyazılıma karşı koruma | **Kontrol**  Kötüamaçlıyazılımakarşıkorumauygulanmalıveuygunkullanıcıfarkındalığı  iledesteklenmelidir. |
| 8.8 | Teknikaçıklıkların yönetimi | **Kontrol**  Kullanımdaolanbilgisistemlerininteknikaçıklıklarıhakkındabilgiedinilmeli, kuruluşun bu açıklara maruz kalma durumu değerlendirilmeli ve uygun önlemleralınmalıdır. |
| 8.9 | Konfigürasyon (yapılandırma)yönetimi | **Kontrol**  Donanım, yazılım, hizmetler ve ağların güvenlik yapılandırmaları da dahil olmak üzere yapılandırmaları oluşturulmalı, doküman haline getirilmeli, uygulanmalı, izlenmeli ve gözden geçirilmelidir. |
| 8.10 | Bilgisilme | **Kontrol**  Bilgisistemlerinde,cihazlardaveyadiğerherhangibirdepolamaortamında saklanan bilgiler, artık gerekli olmadığında silinmelidir. |
| 8.11 | Verimaskeleme | **Kontrol**  Verimaskeleme,ilgilimevzuatdikkatealınarak,kuruluşunkonuyaözgüerişim kontrolüpolitikasıveilgilidiğerkonuyaözgüpolitikalaraveişgerekliliklerine uygun olarak kullanılmalıdır. |
| 8.12 | Verisızıntısıönleme | **Kontrol**  Hassas bilgileri işleyen, depolayan veya ileten sistemlere, ağlara ve diğer tüm cihazlara veri sızıntısı önleme önlemleri uygulanmalıdır. |
| 8.13 | Bilgiyedekleme | **Kontrol**  Bilgilerin, yazılımların ve sistemlerin yedek kopyaları muhafaza edilmeli ve üzerindeanlaşmayavarılankonuyaözgüyedeklemepolitikasınauygunolarak düzenli bir şekilde test edilmelidir. |
| 8.14 | Bilgiişlemetesislerinin  yedekfazlalığı | **Kontrol**  Bilgiişlemeimkanlarında,kullanılabilirlikgerekliliklerinikarşılamakiçin  yeterlimiktardayedeklemesağlanmalıdır. |
| 8.15 | Kaydetme(Logtutma) | **Kontrol**  Faaliyetleri,istisnaları,hatalarıvediğerilgiliolaylarıkaydedenkayıtlar  (loglar)üretilmeli,depolanmalı,korunmalıveanalizedilmelidir. |
| 8.16 | İzlemefaaliyetleri | **Kontrol**  Ağlar,sistemlerveuygulamalaranomaliiçerendavranışlarakarşıizlenmelive potansiyel bilgi güvenliği ihlal olaylarını değerlendirmek için uygun önlemler alınmalıdır. |
| 8.17 | Saatsenkronizasyonu | **Kontrol**  Kuruluştarafındankullanılanbilgiişlemsistemlerininsaatleri,onaylanmış zaman kaynaklarına senkronize edilmelidir. |

16

#### ISO/IEC27001:2022 TSISO/IEC 27001:2022

**ÇizelgeA.1(***devamediyor***)**

|  |  |  |
| --- | --- | --- |
| 8.18 | Ayrıcalıklıdestek  programlarınkullanımı | **Kontrol**  Sistemveuygulamakontrollerinigeçersizkılabilecekdestekprogramların kullanımı kısıtlanmalı ve sıkı bir şekilde kontrol edilmelidir. |
| 8.19 | İşletimsistemlerine yazılım kurulumu | **Kontrol**  İşletimsistemlerindeyazılımkurulumunugüvenlibirşekildeyönetmekiçin  prosedürlerveönlemleruygulanmalıdır. |
| 8.20 | Ağgüvenliği | **Kontrol**  Sistemlerdeki ve uygulamalardaki bilgileri korumak için ağlar ve ağ cihazları güvenlik altına alınmalı, yönetilmeli ve kontrol edilmelidir. |
| 8.21 | Ağhizmetlerinin güvenliği | **Kontrol**  Ağhizmetleriningüvenlikmekanizmaları,hizmetseviyelerivehizmet  gereklilikleribelirlenmeli,uygulanmalıveizlenmelidir. |
| 8.22 | Ağlarınayrımı | **Kontrol**  Kuruluşağlarındabilgihizmetlerigrupları,kullanıcılarvebilgisistemleri ayrılmalıdır. |
| 8.23 | Webfiltreleme | **Kontrol**  Hariciwebsitelerineerişim,kötüamaçlıiçeriğemaruzkalmayıazaltacak şekildeyönetilmelidir. |
| 8.24 | Kriptografi(şifreleme) kullanımı | **Kontrol**  Kriptografikanahtaryönetimidedahilolmaküzerekriptografininetkin  kullanımınayönelikkurallartanımlanmalıveuygulanmalıdır. |
| 8.25 | Güvenligeliştirmeyaşam döngüsü | **Kontrol**  Yazılımvesistemleringüvenlibirşekildegeliştirilmesiiçinkurallaroluşturulmalı ve uygulanmalıdır. |
| 8.26 | Uygulamagüvenlik  gereklilikleri | **Kontrol**  Uygulamalargeliştirilirkenveyaedinilirkenbilgigüvenliğigereklilikleri; tanımlanmalı, belirtilmeli ve onaylanmalıdır. |
| 8.27 | Güvenlisistemmimarisi ve mühendislik ilkeleri | **Kontrol**  Güvenli sistemlerin mühendisliğine yönelik ilkeler oluşturulmalı, dokümante edilmeli, sürdürülmeli ve herhangi bir bilgi sistemi geliştirme faaliyetine uygulanmalıdır. |
| 8.28 | Güvenlikodlama | **Kontrol**  Güvenlikodlamailkeleriyazılımgeliştirmeyeuygulanmalıdır. |
| 8.29 | Geliştirme ve kabul aşamasındagüvenlik testleri | **Kontrol**  Güvenliktestsüreçleri,geliştirmeyaşamdöngüsündetanımlanmalıve uygulanmalıdır. |
| 8.30 | Dışkaynakyoluyla  geliştirme | **Kontrol**  Kuruluş,dışkaynakyoluylasistemgeliştirmeileilgilifaaliyetleriyönetmeli, izlemeli ve gözden geçirmelidir. |
| 8.31 | Geliştirme,testvecanlı (gerçek) ortamlarının ayrılması | **Kontrol**  Geliştirme,testvecanlıortamlarbirbirindenayrılmalıvegüvenlikaltına alınmalıdır. |
| 8.32 | Değişiklikyönetimi | **Kontrol**  Bilgiişlemetesislerivebilgisistemlerindekideğişiklikler,değişiklikyönetimi  prosedürlerinetabiolmalıdır. |
| 8.33 | Testbilgisi | **Kontrol**  Testbilgileriuygunşekildeseçilmeli,korunmalıveyönetilmelidir. |

17

#### TSISO/IEC 27001:2022 ISO/IEC27001:2022

**ÇizelgeA.1(***devamediyor***)**

|  |  |  |
| --- | --- | --- |
| 8.34 | Tetkiktestisırasında bilgi sistemlerinin korunması | **Kontrol**  İşletim sistemlerin değerlendirilmesini içeren tetkik testleri ve diğer güvence faaliyetleri, test uzmanı ve uygun yönetim arasında planlanmalı ve kararlaştırılmalıdır. |

#### ISO/IEC27001:2022 TSISO/IEC 27001:2022

**Kaynaklar**

1. ISO/IEC27002:2022,*Informationsecurity,cybersecurityandprivacyprotection—Information securitycontrols*
2. ISO/IEC27003,*Informationtechnology—Securitytechniques—Informationsecuritymanagementsystems — Guidance*
3. ISO/IEC27004,*Informationtechnology—Securitytechniques—Informationsecuritymanagement — Monitoring, measurement, analysisandevaluation*
4. ISO/IEC27005,*Informationsecurity,cybersecurityandprivacyprotection—Guidanceon managinginformationsecurityrisks*
5. ISO31000:2018,*Riskmanagement—Guidelines*

19