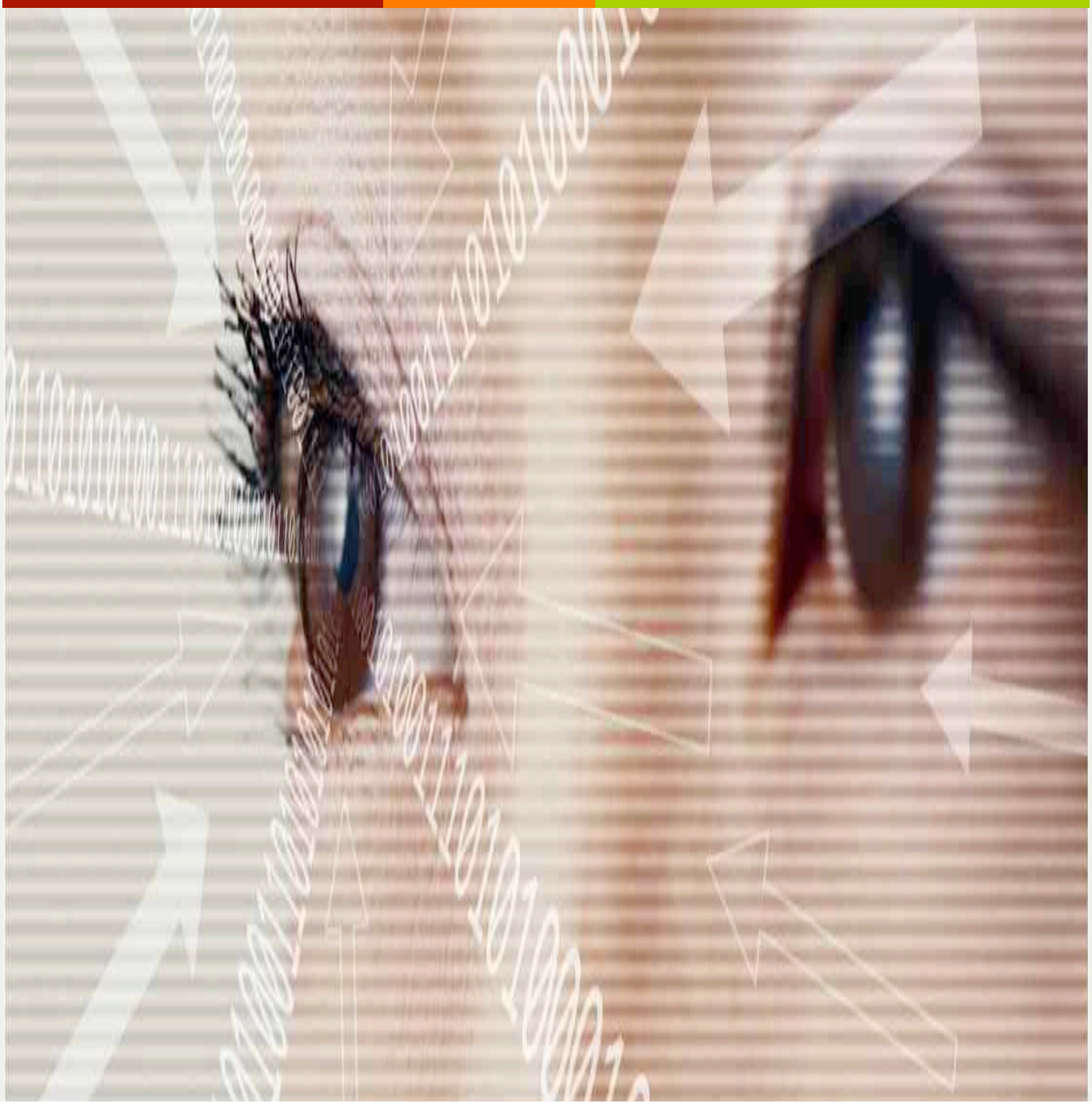
MerSis

Bilgi Güvenliği
Danışmanlık Hizmetleri



Çalışanlarınız, tesisleriniz, üretim araçlarınız koruma altında ! Bilgileriniz ?

Bilgi Güvenliği danışmanlık hizmetlerimiz, en değerli varlıklarınız arasında yer alan bilgilerinizin gizliliğini, doğruluğunu ve erişilebilirliğini güvence altına almak amacıyla geliştirilmiştir.

Günümüzde, bilgi ve destekleyen teknolojiler, kuruluşların en önemli varlıkları arasında kabul edilmektedir. Kritik iş süreçlerinin bilgi ile desteklenmediği sürece verimli çalışmaları mümkün değildir. Üst yönetimlerin hedeflerine ulaşabilmeleri için zamanında ve doğru bilgiye ihtiyaçları vardır. Hassas ve gizli bilgilerin rakiplerin eline geçmesinin doğuracağı sonuçları tahmin etmek bile mümkün değildir.

Başarının ön koşullarından biri olan bilgi, çok çeşitli riskler ile karşı karşıya olmasına rağmen, güvenlik dendiğinde sadece gizlilik ile ilgili riskler çağrışım yapmaktadır. Oysa, yukarıda anımsatıldığı gibi, Bilgi Teknolojileri kesintileri üretim veya hizmet süreçlerinizin tamamen durmasına neden olabilir. Finansal veya operasyonel raporlarınızın yanlış ve/veya tutarsız bilgiler içermesi durumunda, hedeflerinizi doğru belirlemeniz veya isabetli kararlar almanız mümkün olmayacaktır. Yasal düzenlemeler gereği sunmanız gereken raporların zamanında üretilememesi veya yanlış üretilmesi sonucunda sorumlu tutulabilirsiniz. Benzeri nedenlerle müşteri veya iş ortaklarınız ile ilişkilerinizin bozulması söz konusu olabilir. Yaşanabilecek bu tür olumsuzluklar nedeniyle, iş çevrelerinde isminizin kötü anılmaya başlaması ise, belki de geri kazanımı en zor kayıplarınızdan biri olacaktır.

Bilginin iş süreçleri ile olan ilişkisi o denli karmaşık duruma gelmiştir ki, güvenlik ile ilgili riskleri ancak sistematik bir yaklaşım ile yönetebilmek mümkündür. Bilgi güvenliğinin sağlanmasının Bilgi Teknolojileri çalışanlarının sorumluluğu olarak kabul edilmesi, yapılan yaygın hatalardan biridir. Üst yönetimin sorumluluğunda, güvenlik bilincinin tüm kuruluşta yükseltilmesi ve yaygınlaştırılması gerekmektedir. Sadece teknoloji platformları üzerinde alınan önlemlerin yeterli olmadığı bilinmektedir. Geliştirilecek güvenlik önlemlerinin, Kuruluşunuzun kendine özel risklerinin değerlendirildiği bir çalışmanın sonuçlarına göre belirlenmesi gerekmektedir.

Bilgi Güvenliği danışmanlık hizmetlerimiz, Kuruluşunuz bilgilerinin güvenliğini sağlamak üzere, risklerinizin belirlenmesi, güvenlik organizasyonu ve sisteminizin kurulması, güvenlik bilincinin yükseltilmesi amacıyla geliştirilmiştir.

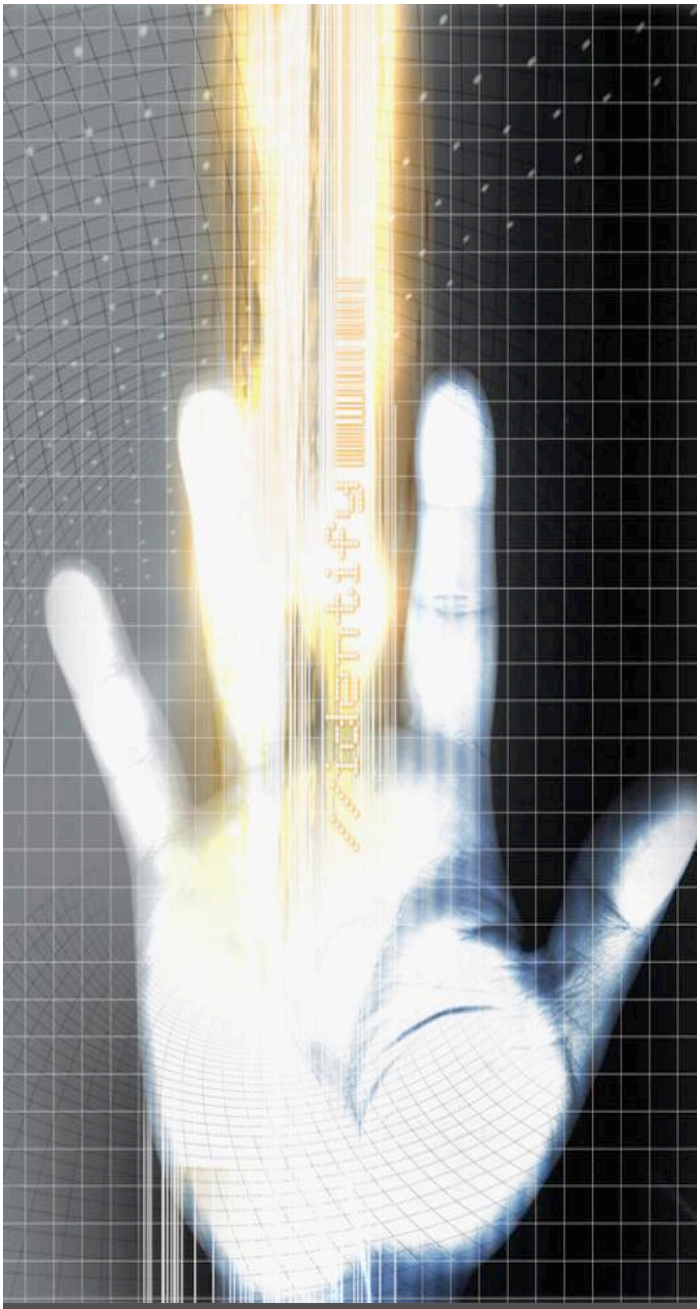
The International Organization for Standardization (ISO) ve The International Electrotechnical Commission (IEC) tarafından yayınlanmış, ISO/IEC 27001:2005(E) Information Management Systems Requirements standartı esas alınarak tasarlanan Bilgi Güvenliği danışmanlık hizmetlerimiz yardımıyla kurulması hedeflenen Bilgi Güvenliği Yönetim Sistemi kapsamında, güvenlik gereksinimlerini 10 ana başlık altında tanımlanmaktadır.

Bilgi Güvenliği Kontrol Hedefleri

ISO/IEC 27001:2005(E) Kontrol Hedefleri

1. Güvenlik Politikası
   - 1.1. Güvenlik Politikası
2. Bilgi Güvenliği Organizasyonu
   - 2.1. İç Organizasyon
   - 2.2. 3. Partiler
3. Varlık Yönetimi
   - 3.1. Varlık Sorumlulukları
   - 3.2. Bilgileri Sınıflandırma
4. İnsan Kaynakları Güvenliği
   - 4.1. İşe Alım Öncesi
   - 4.2. Ç alışma Süresince
   - 4.3. Görev Değişikliği veya Sözleşmenin Sona Ermesi
5. Fiziksel ve Çevre Güvenliği
   - 5.1. Güvenli Alanlar
   - 5.2. Cihaz Güvenliği
6. İletişim ve Operasyon Yönetimi
   - 6.1. İşletimsel Talimatlar ve Sorumluluklar
   - 6.2. Tedarikçi Yönetimi
   - 6.3. Sistem Planlama ve Kabul
   - 6.4. Zararlı Yazılımlara Karşı Koruma
   - 6.5. Yedekleme ve Geri Dönüş
   - 6.6. İletişim Ağları Güvenlik Yönetimi
   - 6.7. Veri Saklama Ortamı Kullanımı ve Güvenliği
   - 6.8. Bilgi paylaşımı ve Güvenliği
   - 6.9. Elektronik Ticaret Hizmetleri
   - 6.10. İzleme
7. Erişim Kontrolü
   - 7.1. Erişim Kontrolü İş Gereksinimleri
   - 7.2. Kullanıcı Erişimi Yönetimi
   - 7.3. Kullanıcı Sorumlulukları
   - 7.4. İletişim Ağları Erişim Kontrolü
   - 7.5. İşletim Sistemleri Erişim Kontrolü
   - 7.6. Uygulama ve Bilgi Erişimi Kontrolü
   - 7.7. Mobil Bilgi İşlem ve Kablolu İletişim
8. Bilgi Teknolojileri Edinme, Geliştirme ve Bakım
   - 8.1. Sistemlerin Güvenlik Gereksinimleri
   - 8.2. Uygulama Sistemlerinin Güvenliği
   - 8.3. Şifreleme Kontrolleri
   - 8.4. Sistem Dosyalarının Güvenliği
   - 8.5. Geliştirme ve Destek Süreçlerinin Güvenliği
   - 8.6. Teknik Güvenlik Açıklarının Yönetimi
9. Güvenlik Olayları Yönetimi
   - 9.1. Güvenlik Olayları ve Açıklarının Raporlanması
   - 9.2. Güvenlik Olayları Yönetimi ve İyileştirme
10. İş Sürekliliği Yönetimi
    - 10.1.İş Sürekliliği Yönetiminde Bilgi Güvenliği
11. Uygunluk
    - 11.1.Yasal Gereksinimler ile Uyum
    - 11.2.Güvenlik Politikaları, Standartlar ve Teknik Gereksinimler ile Uyum
    - 11.3.Denetim Esasları

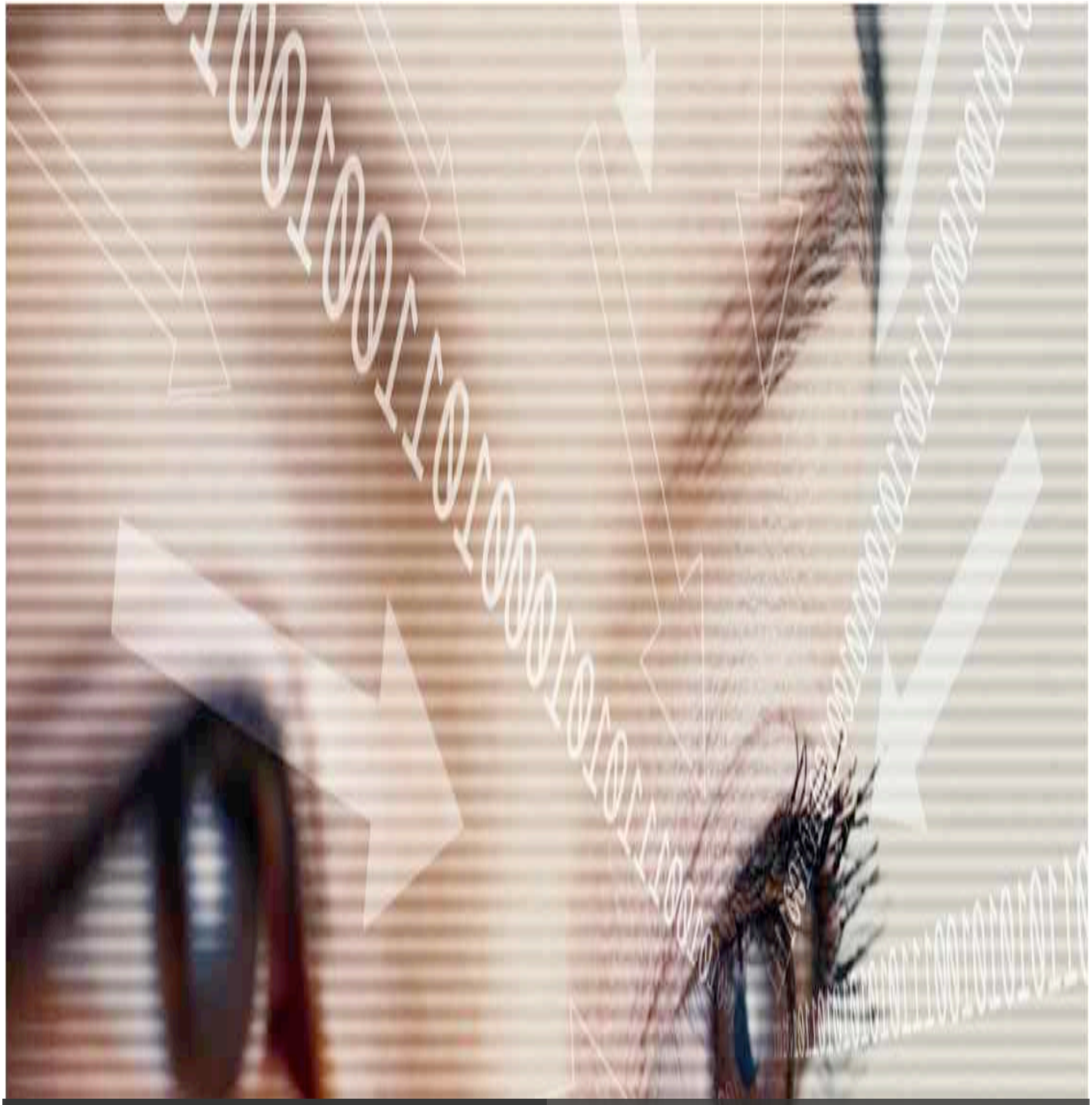
Bilgi Güvenliği danışmanlık hizmetlerimiz, ISO/IEC 27001:2005(E) standartı kapsamında önerildiği şekilde, planlama, uygulama, gözden geçirme ve iyileştirme faaliyetlerini içeren 4 aşamada sunulmaktadır.



Bilgi Güvenliği Yönetim Sistemi Uygulama Metodolojisi

- **Bilgi Güvenliği Yönetimi Sisteminin (BGYS) Kurulması**
  - Kuruluşunuzun gereksinimleri doğrultusunda BGYS kapsam ve kısıtları belirlenir.
  - BGYS politikalarınız tanımlanır.
  - Risk değerlendirme yaklaşımlarınız ve metodoloji belirlenir.
  - Riskleriniz tanımlanır.
  - Riskleriniz analiz edilir ve değerlendirilir.
  - Risklerinize karşı gerekli önlemler tanımlanır, alternatifler değerlendirilir.
  - Önlemlerin uygulanmasını güvence altına almak üzere gerekli kontrol hedefleri ve kontrollar belirlenir.
  - Önlemler sonucunda kalacak risk düzeyleri için yönetim onayı alınır.
  - BGYS uygulamaları için yönetimin onayı alınır.
  - ISO 27001 standartları ile uyum beyanı hazırlanır.

- **BGYS'nin Uygulanması**
  - Güvenlik önlemlerini uygulamaya geçirmek üzere gerekli faaliyetler, kaynaklar, sorumluluklar ve öncelikler planlanır.
  - Kontrol hedeflerine ulaşmak üzere planlar uygulanır.
  - Uygulamaların etkinliğini ölçmek için gerekli kriterler tanımlanır.
  - Gerekli eğitimler sağlanır ve güvenlik bilincini yükseltme programları uygulanır.
- **BGYS Uygulamalarının İzlenmesi ve Gözden Geçirilmesi**
  - Uygulamalar sırasında karşılaşılan hatalar tespit edilir.
  - Güvenlik saldırıları ve olayları tespit edilir.
  - Uygulamalar ve sonuçları yönetime raporlanır.
  - Güvenlik olaylarını çözümlemek üzere alınan önlemlerin etkinliği değerlendirilir.
  - BGYS etkinliği düzenli olarak gözden geçirilir.
  - Risk değerlendirmeleri düzenli olarak gözden geçirilir.
  - BGYS düzenli olarak denetlenir.
  - BGYS düzenli olarak yönetim ile birlikte gözden geçirilir.
  - Uygulama planları, gözden geçirme sonucu alınan kararlar ışığında güncellenir.
- **BGYS Güncellenmesi ve İyileştirilmesi**
  - BGYS kapsamında belirlenen iyileştirmeler uygulamaya alınır.
  - Düzeltici ve önleyici faaliyetler takip edilir.
  - İyileştirme faaliyetleri ile ilgili tüm taraflar bilgilendirilir.
  - İyileştirme faaliyetlerinin beklenen hedeflere ulaştığı test edilir.



MerSis Bilgi Teknolojileri Danışmanlık Ltd.

Atatürk Cad. Ulaştırıcı Sok. No:3
Eriş Sitesi A Blok Daire:18
Kozyatağı 34736
Kadıköy-İstanbul
Tel : +90 (216) 302 87 95 (pbx)
Fax : +90 (216) 302 8920

www.mersis.com.tr