Eğitimlerimiz

ISO/IEC 27001 BİLGİ GÜVENLİĞİ YÖNETİM SİSTEMİ TEMEL EĞİTİMİ:

Kurs Tanımı:

Son zamanlardaki üst düzey bilgi güvenliği ihlalleri ve bilginin değeri, şirketlerin bilgilerini korumaya yönelik giderek artan ihtiyacı vurgulamaktadır. Bilgi Güvenliği Yönetim Sistemi (BGYS), hassas şirket bilgilerinin güvenli kalmasına yönelik kontrollü bir idari yaklaşımdır. Kişileri, süreçleri ve Bilgi Yönetimi Güvenlik Sistemlerini kapsar.

ISO/IEC 27001 Bilgi Teknolojisi - Güvenlik Teknikleri-Bilgi Güvenliği Yönetim Sistemleri - Gereksinimler Standardı'nın kurum ve kuruluşlarda tesis edilmesi için yapılacak çalışmaların başlangıcında, kurumun bilgi işlem faaliyetlerini yürüten bilgi işlem personeli içerisinden belirlenen ve standardizasyon faaliyetlerinde doğrudan görev alacak personele verilen bir eğitimdir.

Bu kursun amacı, katılımcılara, ISO 27002 şartlarına uygun ve ISO 27001: 2013'in sertifikasyon kriterlerini karşılayan bir BGYS uygulamaları için gerekli becerileri kazandırmaktır. Bu kurs, katılımcılara bir uygulama çerçevesi sunar.

Kimler katılmalı?

- ISO 27001: 2013 Bilgi güvenliği yönetim sisteminin uygulanmasıyla ve idaresiyle görevli personel,
- Bilgi güvenliği danışmanları.

İşinize faydası:

Kursun amacı uzman eğitmenin önderliğiyle ve verdiği eğitimle etkili bir BGYS'nin kurulması olacaktır. Bu çalışma sırasında edindiğiniz bilgi ve becerileri, işinizi geliştirmek ve korumak için kullanabilirsiniz.

Kurs yapısı:

- Bilgi Güvenliğinin geçmişi,
- Bilgi Güvenliği politikasının kapsamının belirlenmesi,
- Bilgi varlıklarının tanımlanması,
- Bilgi varlıklarının değerinin belirlenmesi,
- Risk ve etkilerin belirlenmesi,
- Kontrol hedeflerinin ve kontrollerin tanımlanması,
- Politikaların tanımlanması ve uygulanması,
- Politikaların, standartların ve prosedürlerin oluşturulması ve uygulanması,
- BGYS belgeleme gerekliliklerinin tamamlanması,
- Farkındalık eğitimi,
- Belgelendirme süreci,
- Bir BGYS Projesi Uygulama Planının oluşturulması.

Kurs süresi:

3 gün

ISO/IEC 27002 UYGULAMA EĞİTİMİ:

Kurs Tanımı:

Bilgi güvenliği hem sizin için hem de müşterileriniz için çok büyük önem taşır. Uluslararası Bilgi Güvenliği Yönetimi Standardını (ISO 27001:2013) tüm ticari açılardan derinlemesine inceleyen bir günlük kapsamlı bir eğitimdir.

Eğitim kapsamında; ISO/IEC 27001 Standardının temel gereksinimleri ile ISO/IEC 27001 Standardının EK-A'sında belirtilen kontrol maddelerinin her biri için ISO/IEC 27002 Bilgi Teknolojileri – Güvenlik Teknikleri – Bilgi Güvenliği Yönetimi için Pratik Uygulamalar Standardında belirtilen uygulama şekilleri hakkında bilgi verilmektedir.

Katılımcılar şu konular hakkında bilgi edinir;

- Bilgi güvenliği,
- Standardın amacı,
- Kontrol amaçları ve kontroller,
- En temel kontrollerin önemi,
- Bir kuruluşa ISO 27001:2013'i uygulamanın etkileri,
- Belgelendirme ve ticari baskıların etkileri,
- Uygunsuzluğa yönelik cezalar.

Kimler katılmalı?

- Üst Düzey Yöneticiler,
- Bilgi Güvenliği Yöneticileri,
- Sistem Yöneticileri,
- İş Sürekliliği Yöneticileri,
- Bir kuruluşa ISO 27001:2013 standardını getirmekle yükümlü tetkikçiler.

İşinize faydası:

- Tüm kurum genelinde etkili bir bilgi güvenliği yönetimi,
- Sizin ve müşterilerinizin çıkarlarının kusursuz biçimde korunması.
- Kurs yapısı
- Bilgi Güvenliğine giriş: Temel konular, söylentiler ve gerçekler,
- İş Gereklilikleri: Ticari ve yasal hususlar,
- BGYS (Bilgi Güvenliği Yönetim Sistemi) standartlarına giriş: Tarihi, gelişimi ve mevcut durumu,
- Bir yönetim sisteminin geliştirilmesi ve uygulanması,
- Politika,
- Kapsam,
- Risk Değerlendirmesi,
- Risk Yönetimi,

- Uygulanabilirlik Bildirisi,
- Önemli Başarı Faktörleri,
- Açık Tartışma.

Kurs süresi:

1 gün

IRCA Onaylı ISO/IEC 27001 İç Tetkikçi Eğitimi:

Kurs Tanımı:

ISO/IEC 27001 Standardı gereğince kurum içi denetimleri gerçekleştirilecek personel için verilen iki gün süreli eğitimdir.

Kimler katılmalı?

ISO 27001: 2013 Bilgi güvenliği yönetim sisteminin uygulanmasıyla ve idaresiyle görevli personel.

İşinize faydası:

Kursun sonunda belgelendirilen personel yardımıyla ISO/IEC 27001 gereğince yılda asgari bir kez yapılması gereken iç denetim faaliyetini gerçekleştirebiliyor olacaksınız.

Kurs yapısı:

Eğitim kapsamında iç tetkik öncesi hazırlıklar, denetimin icrası ve raporlama konularında uygulamalı olarak bilgi verilmekte ve başarılı katılımcılara International Register of Certificated Auditors (IRCA) onaylı "İç Tetkikçi Belgesi" firmamız tarafından verilmektedir.

Kurs süresi:

2 gün.

ISO/IEC27005 RİSK DEĞERLENDİRMESİ EĞİTİMİ:

Kurs Tanımı:

ISO/IEC 27001 standardının gereği Kuruluşun risk değerlendirme yaklaşımının tanımlanma maddesine sistematik yaklaşımın ilk adımıdır.

Kuruluş ve tanımlanmış iş bilgisi güvenliğine, yasal ve düzenleyici gereksinimlere uygun bir risk değerlendirme metodolojisi tanımlamak, Riskleri kabul etmek için kriterler geliştirme ve kabul edilebilir risk seviyelerini tanımlamak ve riskleri kabul etme ölçütlerini ve kabul edilebilir risk seviyelerini belirlemek zorundadır.

Kimler katılmalı?

Her kademedeki yöneticiler ile ISO 27001 Bilgi Güvenliği Yönetim Sistemi'ni planlamak, kurmak ve uygulamakla sorumlu personel.

İşinize faydası:

- BGYS standartlarının ve bunların uygulanmasının iyice anlaşılması,
- Şirketinizi en iyi BGYS uygulamalarıyla karşılaştırabilme becerisi,
- Kuruluşunuzda BGYS'nin uygulanması için net bir strateji.

Kurs yapısı:

- Giriş,
- Yasal gereklilikler,
- Varlıkları belirlenmesinde ekonomik kayıplar yaklaşımı,
- Önem derecelendirmesinin gerekliliği,
- Önemli risklerin belirlenmesi için puanlama,
- Kontroller ve Düzeltici faaliyetler.

Kurs süresi:

1 gün

BİLGİ GÜVENLİĞİ FARKINDALIK EĞİTİMİ:

Kurs Tanımı:

ISO/IEC 27001 Bilgi Güvenliği Yönetim Sistemi kurulum danışmanlığı kapsamında veya gereksinim duyulan durumlarda kurum ve kuruluşların tüm çalışanlarına verilen iki saat süreli eğitimdir.

Eğitim kapsamında kurum ve kuruluşlarda bilgi güvenliği standartlarına uyumluluğun sürekliliğini sağlamak amacıyla tüm çalışanların uyması gereken kurallar hakkında bilgi verilmektedir.

Kimler katılmalı?

Tesis edilen bilgi güvenliği yönetim sistemi kapsamındaki tüm çalışanlar.

İşinize faydası:

- BGYS standartlarının ve bunların uygulanmasının tüm personel tarafından iyice anlaşılması,
- Güvenlik ihlâl olaylarının yönetimi sürecinde çalışanlarca yapılması gereken faaliyetler.

Kurs yapısı:

- Bilgi sistemlerinin güvenli kullanımı,
- Çalışanların uyması gereken kurallar,
- İhlâl olayları bildirimi.

Kurs süresi:

2 Saat.

KURUM VE KURULUŞLARIN ÜST DÜZEY YÖNETİMİ İÇİN BİLGİ GÜVENLİĞİ YÖNETİMİ EĞİTİMİ:

Kurs Tanımı:

Üst düzey yönetimi bilgi güvenliği konusunda bilgilendirmek, yönlendirmek ve farkındalığı artırmak amacıyla verilen iki saat süreli eğitimdir.

Kimler katılmalı?

Kurumun üst düzey yöneticileri.

İşinize faydası:

- Yöneticilerin Bilgi Güvenliği konusunda farkındalıkları geliştirilir,
- Güvenlik gereksinimlerinin yerine getirilmesinde üst yönetim desteği artırılır.

Kurs yapısı:

Eğitim kapsamında üst yönetimle ilgili bilgi güvenliğine yönelik politika, strateji ve yönetimin gözden geçirmesi konularında bilgi verilmektedir.

Kurs süresi:

2 Saat.

BS 10012 - KİŞİSEL BİLGİ YÖNETİM SİSTEMİ İÇİN VERİ KORUMA STANDARDI EĞİTİMİ:

Kurs Tanımı:

Kurum/Kuruluşlarda saklanan/işlenen kişisel bilgilerin gizlilik, bütünlük ve erişilebilirliğinin sürekliliğini sağlamak amacıyla tesis edilecek BS 10012 Standardının uygulanmasına yönelik gereksinimlere ilişkin bilgilerin verildiği eğitimdir.

Veri koruması ve güvenlik konuları kurumlar için gittikçe daha kritik hale gelmektedir. Bunun için kurumlarda Kişisel Bilgi Yönetim Sistemleri (KBYS) - Personal Information Management System (PIMS) kurulmaktadır. BS 10012; bu sistemlerle ilgili standartları belirlemektedir.

PIMS ilkelerinin oluşturulması, PIMS'nin kurum kültürüne sokulması, uyumun sağlanması için yapılması gerekenler BS 10012'nin kapsamını oluşturmaktadır.

Eğer kurumunuz KEPHS (Kayıtlı Elektronik Posta Hizmet Sağlayıcısı) olmak istiyorsa BS 10012 standardına sahip olmalıdır veya sahip olabileceğini taahhüt etmelidir. BTK'nın ilgili yönetmeliği bunu gerektirir. Yönetmeliğin zorunlu kıldığı bir diğer standart ise ISO/IEC 27031'dir.

Kimler katılmalı?

Kurumdaki kişisel bilginin yönetiminden sorumlu tüm personel.

İşinize faydası:

- Kişisel bilgilerin korunmasına yönelik standart uygulamalar,
- Kurumun kişisel bilgi güvenliğine yönelik olarak edindiği rekabet ve güven ortamı.

Kurs yapısı

Kişisel bilgi yönetim sistemi nedir?

- Kişisel Bilgi Koruma Prensipleri nelerdir?
- Hassas kişisel bilgiler nelerdir?
- Kişisel Bilgi Sistemi (KBYS)'nin planlanması,
- KBYS'nin kurulumu ve yönetimi,
- KBYS'nin kapsamı ve hedefleri,
- KBYS Politikası.

KBYS'nin uygulanması ve işletilmesi;

- Kişisel bilgi kullanımının belirlenmesi ve kaydedilmesi;
- Yüksek riskli kişisel bilgiler,
- Eğitim ve farkındalık yaratma,
- Risk belirleme ve işleme,
- Doğru ve yasal işleme,
- Kişisel bilginin toplanması ve işlenmesi kuralları,
- Üçüncü taraflarca paylaşımda sorumluluklar,
- Veri paylaşım şartları,
- Yeterli, ilgili ve aşırı olamayan kişisel bilgi,
- Saklama ve yok etme,
- Bireylerin hakları,
- Kişisel bilginin Avrupa Ekonomik Alanı'nın dışına iletilmesi,
- KBYS'nin izlenmesi ve gözden geçirilmesi.

İç denetim,

Yönetimin gözden geçirmesi,

KBYS'nin geliştirilmesi;

- Önleyici ve düzeltici faaliyetler.

Kurs süresi:

1 gün.

ISO/IEC 27799 - SAĞLIK İNFORMATİĞİ - ISO/IEC 27002 KULLANILARAK SAĞLIKTA BİLGİ GÜVENLİĞİ YÖNETİMİ STANDARDI EĞİTİMİ:

Kurs Tanımı:

Sağlık Sektöründe saklanan/işlenen kişisel sağlık bilgilerinin gizlilik, bütünlük ve erişilebilirliğinin sürekliliğini, kurumlar ve ülkeler arasında sağlık bilgisinin değişim esaslarına yönelik standartlarla uyumu sağlamak amacıyla tesis edilecek ISO/IEC 27799 Standardının gereksinimlerine ilişkin bilgilerin verildiği eğitimdir.

Kimler katılmalı?

- Sağlık bilgi güvenliği sorumluları,
- Sağlık bilgi güvenliği danışmanları,
- Denetçiler,
- Üçüncü taraf hizmet sağlayıcıları.

İşinize faydası:

Sağlık kuruluşlarında saklanan/işlenen kişisel sağlık bilgisinin gizliliğini, bütünlüğünü ve sürekli erişilebilirliğini uluslararası standartta sağlamak ve sürdürmek.

Kurs yapısı:

- ISO/IEC 27002 kullanılarak Sağlık bilgi güvenliğinin sağlanması,
- ISO/IEC 27799 ile ek açıklama getirilen kontrol maddelerinde belirtilen konular.

Kurs süresi:

1 Gün.

ISO/IEC 27011 - BİLGİ TEKNOLOJİLERİ-GÜVENLİK TEKNİKLERİ-TELEKOMÜNİKASYON KURULUŞLARI İÇİN ISO/IEC 27002 TABANLI BİLGİ GÜVENLİĞİ YÖNETİM REHBERİ STANDARDI EĞİTİMİ:

Kurs Tanımı:

Telekomünikasyon Sektöründe saklanan/işlenen bilgilerin gizlilik, bütünlük ve erişilebilirliğinin sürekliliğini sağlamak amacıyla özellikle bu sektörde alınması gereken güvenlik önlemlerini dikkate alan ISO/IEC 27011 Standardının gereksinimlerine ilişkin bilgilerin verildiği eğitimdir.

Kimler katılmalı?

- Telekomünikasyon sektörü bilgi güvenliği sorumluları,
- Telekomünikasyon sektörü bilgi güvenliği danışmanları,
- Denetçiler,
- Üçüncü taraf hizmet sağlayıcıları.

ISO/IEC 27019 - BİLGİ TEKNOLOJİLERİ-GÜVENLİK TEKNİKLERİ-ENERJİ ALTYAPILARI İÇİN BİLGİ GÜVENLİĞİ EĞİTİMİ:

Kurs Tanımı:

Telekomünikasyon Sektöründe saklanan/işlenen bilgilerin gizlilik, bütünlük ve erişilebilirliğinin sürekliliğini sağlamak amacıyla özellikle bu sektörde alınması gereken güvenlik önlemlerini dikkate alan ISO/IEC 27011 Standardının gereksinimlerine ilişkin bilgilerin verildiği eğitimdir.

Kimler katılmalı?

- Enerji Sektörü Sistem Planlama Uzmanları, Sektör Yöneticileri, Proses Kontrol Çalışanları ve Süreç Yönetim Uzmanları.
- Enerji sektörü bilgi güvenliği sorumluları,
- Denetçiler,
- Üçüncü taraf hizmet sağlayıcıları.

İşinize faydası:

Enerji üreten ve ileten kuruluşlarda saklanan/işlenen kişisel sağlık bilgisinin gizliliğini, bütünlüğünü ve sürekli erişilebilirliğini uluslararası standartta sağlamak ve sürdürmek.

Kurs yapısı:

- ISO/IEC 27002 kullanılarak Enerji sektöründe bilgi güvenliğinin sağlanması,
- ISO/IEC 27019 ile ek açıklama getirilen ve yeni eklenen kontrol maddelerinde belirtilen konular.

Kurs süresi:

1 Gün.

ISO/IEC 27031 - BİLGİ TEKNOLOJİLERİ-GÜVENLİK TEKNİKLERİ-İŞ SÜREKLİLİĞİ İÇİN BİLGİ VE İLETİŞİM TEKNOLOJİLERİ HAZIRLIK PRENSİPLERİ STANDARDI FARKINDALIK EĞİTİMİ:

Kurs Tanımı:

Katılımcılara İş Sürekliliği Yönetimini (İSY) ve BSI tarafından çıkarılan yeni ISO/IEC 27031 standardına ilişkin kapsamlı bir anlayış sunar. Pratik egzersizler ve eğitmen yönetimindeki tartışmalar, öğrencilerin bu 1 günlük eğitimde bir 27031 uygulama projesi başlatmak için hangi koşulların gerektiğini anlamlarını sağlar ve 27031 ve bir iş sürekliliği yönetim sistemini uygulamaya yönelik kararı konusunda şirketlerine yön göstermelerini sağlar.

Tüm sektörlerde bilgi teknolojilerine olan bağımlılık dikkate alınarak iş sürekliliğinin sağlanmasına yönelik olarak yerine getirilmesi gereken tüm faaliyet ve tedbirleri belirleyen ISO/IEC 27031 Standardının gereksinimlerine ilişkin bilgilerin verildiği eğitimdir.

Mart 2011'de yayımlanan ISO/IEC 27031:2011 standardı; kurumların iş sürekliliğinin sağlanması konusundaki gereksinimleri içeriyor. Bu standardın içeriği/amacı özet olarak;

- Özel sektör veya devlet kurumlarına iş sürekliliğinin sağlanması konusunda süreçler ve mimariler önermek,
- Kurumlardaki BGYS'ye (Bilgi Güvenliği Yönetim Sistemi) destek olmak. Performans kriterlerini de göz önüne alarak tasarım ve uygulama konusundaki gereklilikleri tanımlamak. Bu tanımlamalardaki amaç yine iş sürekliliğidir. Yalnızca güvenlik ile ilgili standartlar bulunmamaktadır.
- Felaketlere karşı organizasyonun direncini arttırmayı hedefler. Süreklilik, güvenlik ve felaketlere karşı hazırlıklı olmaktır.

Eğer kurumunuz KEPHS (Kayıtlı Elektronik Posta Hizmet Sağlayıcısı) olmak istiyorsa BTK'nın ilgili yönetmeliğin zorunlu kıldığı bir diğer standart ise ISO/IEC 27031'dir.

Aşağıdaki sertifikasyonlara sahip olan kurumlar aslında bu standarda da bir şekilde dâhil olmuş durumdalar. Birbirlerini tamamlayıcı nitelikte standartlar diyebiliriz;

- ISO/IEC 27001,
- ISO 2239PAS,
- ISO 23301.

Kimler katılmalı?

- İş Sürekliliği yöneticileri,
- Risk yöneticileri,
- Kalite müdürleri,
- BT müdürleri,
- Bilgi Güvenliği uzmanları,
- Bir kuruluşa 27031 standardını getirme konusuna dahil olacak uzmanlar,
- İş sürekliliği operasyonlarını denetleyecek tetkikçiler.

Amaç:

Bu kursu tamamladıktan sonra katılımcılar şunları yapabiliyor olmalıdır:

- Kurumlarındaki iş sürekliliğine yönelik tehlikeleri analiz etmek ve tanımlamak,
- Tehlikeleri ve olası etkilerini öncelik sırasına koymak,
- İş sürekliliği seçeneklerini belirlemek,
- İş sürekliliğini sağlayacak bir tepki uygulamak,
- İş Sürekliliği Planının nasıl uygulanacağını ve sürdürüleceğini tanımlamak,
- 27031 in diğer standartlarla ilişkisini açıklamak.

Gerekli Ön Bilgi:

Resmi bir ön koşul olmamakla birlikte, öğrencilerin iş uygulamaları ve yönetim sistemleri hakkında genel bir bilgi sahibi olmaları tavsiye edilir.

Kurs süresi:

1 Gün.

ADLİ BİLİŞİM EĞİTİMİ:

Kurs Tanımı:

Adli Bilişim Eğitimi güncel teknolojileri ve yöntemleri kapsamakta olup, eğitim çoğunlukla teorik bilgileri destekleyen ve bu bilgilerin pekiştirilmesini sağlayan uygulamalarla verilmektedir. İnceleme esnasında edinilen delillerin geçerliliğinin bozulmadan ve değiştirilmeden raporlanıp adli mercilere sunulması süreçlerini kapsar. Eğitim uluslararası geçerli sertifikasyona sahip eğitmenler tarafından verilmektedir.

Kimler katılmalı?

Adli bilişimle ilgili delil elde etmekle görevlendirilecek personel.

İşinize faydası:

Herhangi bir ihlâl olayında edinilen delillerin geçerliliğinin bozulmadan ve değiştirilmeden raporlanıp adli mercilere sunulmasını sağlar.

Kurs yapısı:

- Dijital deliller ve adli bilişim,
- Dijital delillere el koyma ve imaj kopya alma süreçleri,
- Adli bilişim laboratuvarları,
- Adli bilişim incelemelerinde kullanılan araç-gereçler;
  - Donanımlar,
  - Yazılımlar,
  - Metotlar.
- Laboratuvar incelemelerinde neler tespit edilebilir?
- Hard disklerin incelenmesi,
- Hard disklere veri nasıl yazılır ve silinir?
- Kalıcı silme (wipe) uygulamaları,
- Veri kurtarma;
  - Silinen bilgiler nasıl kurtarılır?
  - Silinmiş partition'dan veri kurtarma,
  - Format sonrası veri kurtarma,
  - Silme komutu sonrası silinen verilerin kurtarılması,
- Gizlenmiş bilgilerin tespiti,
- Şifrelenmiş bilgilerin tespiti,
- Facebook, Twitter, Msn vb. sosyal ağlardan yazışma kayıtlarının tespiti,
- Cep telefonları ve adli bilişim incelemeleri;
  - Arama kayıtları,
  - Cep telefonu ile çekilmiş görüntüler,
  - Fotoğrafın hangi telefon ile çekildiğinin tespiti,
  - Silinmiş ses kayıtlarının kurtarılması,
  - Bir cep telefonuna geçmişte takılmış olan SIM kartların tespiti,
- Optik medya (CD-DVD) ve adli bilişim incelemeleri;

- CD'nin oluşturulma tarihi,
- CD'den silinmiş kayıtların kurtarılması,
- CD'lerden veri kurtarma,

- Dijital kayıtlarda saat-tarih incelemesi;
  - Dosyaların tarih-saat bilgileri ne anlama gelir?
  - Dosya tarih-saatlerinin değişmesi/değiştirilmesi mümkün mü?
  - Dosya tarih-saatleri ne kadar güvenilirdir?
  - Bilgisayar ortamında tarih-saat bilgilerinin ispat gücü nedir?
- Msn, facebook vb. ortamlardan silinmiş ve geçmişe yönelik görüşme kayıtlarının tespiti,
- Hafıza kartlarının incelenmesi,
- Metadata (Üst veri) incelemesi;
  - Yazıcıdan alınan bir dokümanın incelenmesi, alınma zamanının incelenmesi,
  - Bir resim hangi marka-model makine ile çekildi, nerede çekildi bilgilerinin tespiti,
  - Bir dosyayı ilk oluşturan kullanıcı profili bilgilerinin tespiti,
  - Windows kayıt defteri (registry) incelemesi;
  - Bilgisayara takılmış olan USB belleklerin tespiti,
  - İnternette son aratılan sözcükler listesi,
- Encase ile adli bilişim incelemesi;
  - İnternet bankacılığı yoluyla dolandırıcılık,
  - Kontör dolandırıcılığı,
  - Bilişim sistemleri üzerinden hakaret, sövme, tehdit, şantaj suçları,
  - Kopya yazılım, fikri mülkiyet haklarının ihlali,
  - Özel hayatın gizliliğinin ihlali,
  - İnternette kişisel verilerin yayınlanması,
  - Bilişim sistemlerine yetkisiz erişim ve bilişim sistemlerini bozma,
  - İnternette çocuk pornografisi,
  - Başkalarına ait msn, facebook, e-mail hesaplarının ele geçirilmesi,
  - Bilişim sistemleri yoluyla sahtecilik,
  - Suç içerikli siteler ve kaynak tespiti,
  - IP tespiti ve kişiye ulaşma,
- Bilişim bilirkişi raporları ve güvenilirliği.

Kurs süresi:

5 Gün.