# NIST Cybersecurity Foundation Eğitimi

Süre: **2 Gün**

BİLGİNÇ IT Academy
info@bilginc.com
bilginc.com

Bu Eğitim Size Ne Kazandırır?

- **NIST siber güvenlik standartlarını ve çerçevelerini** tanıyarak kuruluşunuzun güvenlik çalışmalarına daha bilinçli katkıda bulunabilirsiniz.
- **Siber güvenlik risklerini, tehditleri ve güvenlik açıklarını** belirlemeye yönelik temel yaklaşımları öğrenebilirsiniz.
- **NIST Cybersecurity Framework (CSF) 2.0** ve **NIST Risk Management Framework (RMF)** yapılarını anlayarak güvenlik süreçlerini değerlendirebilirsiniz.
- **İdari, teknik ve fiziksel güvenlik kontrollerinin** riskleri azaltmadaki rolünü kavrayabilirsiniz.
- **Siber güvenlik farkındalığı, olay müdahalesi ve kurumsal dayanıklılık** konularında temel bilgi kazanabilirsiniz.
- **NIST rehberlerini gerçek iş senaryolarına uygulayarak** güvenlik yönetişimi, risk yönetimi ve iyileştirme çalışmalarını destekleyebilirsiniz.

**NIST Cybersecurity Foundation Eğitimi**, **NIST (National Institute of Standards and Technology)** tarafından geliştirilen siber güvenlik ilkelerini, standartlarını ve rehberlerini temel düzeyde öğrenmek isteyen katılımcılar için hazırlanmış **2 günlük bir eğitim programıdır**.

Eğitim, kuruluşların siber güvenlik risklerini anlamalarına, uygun güvenlik kontrollerini değerlendirmelerine ve kurumsal güvenlik programlarının uygulanmasına katkı sağlamalarına yardımcı olmayı amaçlar.

Program kapsamında **siber güvenliğin temel kavramları, NIST yayınları, risk yönetimi, güvenlik kontrolleri, güvenlik farkındalığı ve olay yönetimi** konuları ele alınır. Katılımcılar, bilgi varlıkları, tehditler, güvenlik açıkları ve riskler arasındaki ilişkileri öğrenirken bu kavramların kurumsal karar alma süreçlerinde nasıl kullanıldığını inceler.

Eğitimde **NIST SP 800-12, NIST SP 800-53, NIST SP 800-37 ve NIST SP 800-171** yayınlarının amaçları açıklanır. Ayrıca **NIST Cybersecurity Framework (CSF) 2.0** çerçevesinin yapısı ve kuruluşların güvenlik olgunluğunu geliştirmedeki rolü değerlendirilir.

**NIST Risk Management Framework (RMF)** kapsamında risk yönetiminin yaşam döngüsü ve güvenlik kontrolleriyle ilişkisi incelenir. Katılımcılar, **Prepare, Categorise, Select, Implement, Assess, Authorise ve Monitor** aşamalarının temel amaçlarını öğrenir.

Eğitimin diğer bölümlerinde **Controlled Unclassified Information (CUI)** olarak sınıflandırılan hassas bilgilerin korunması, çalışan farkındalığı, güvenlik sorumlulukları ve olay müdahale süreçleri üzerinde durulur.

Program, **senaryo temelli uygulamalarla** NIST yayınlarının kurumsal güvenlik faaliyetlerinde nasıl kullanılabileceğini gösterir. Böylece katılımcılar, **risklerin belirlenmesinden güvenlik kontrollerinin uygulanmasına, izleme ve olay müdahalesinden sürekli iyileştirmeye** uzanan bütünsel bir bakış açısı kazanır.

# NIST Cybersecurity Foundation Eğitimi

Süre: **2 Gün**

BİLGİNÇ IT Academy
info@bilginc.com
bilginc.com

### Sınav ve Değerlendirme

Eğitim kapsamında **siber güvenliğin temel ilkeleri, risk yönetimi ve güvenlik kontrolleri** konularını kapsayan bir **sertifikasyon sınavı** bulunmaktadır.

## Önkoşullar

Bu eğitime katılmak için **herhangi bir ön koşul bulunmamaktadır**.

Program, siber güvenlik ve NIST rehberleri hakkında temel bilgi edinmek isteyen katılımcılara uygundur.

## Kimler Katılmalı

Eğitim, **NIST tabanlı siber güvenlik yaklaşımlarını öğrenmek** ve kuruluşların bilgi güvenliği faaliyetlerine katkıda bulunmak isteyen profesyonellere yöneliktir.

Özellikle:

- Kuruluşlarında **siber güvenlik çalışmalarını desteklemekten** sorumlu yöneticiler, danışmanlar ve ekip liderleri
- **Siber güvenlik veya bilgi güvenliği faaliyetlerinde** görev alan ve iyi uygulamaları öğrenmek isteyen çalışanlar
- **Siber güvenlik yönetişimi, risk yönetimi ve olay müdahalesi** alanlarında bilgi birikimini geliştirmek isteyen profesyoneller
- **Siber güvenlik alanında kariyere başlamayı** veya NIST rehberlerini daha iyi anlamayı hedefleyen kişiler
- **Güvenli sistemlerin kurulumu ve sürdürülmesini** destekleyen BT personeli ve sistem yöneticileri

# NIST Cybersecurity Foundation Eğitimi

Süre: **2 Gün**

BİLGİNÇ IT Academy
info@bilginc.com
bilginc.com

## Neler Öğreneceksiniz

Bu eğitimi tamamladığınızda:

- **Siber güvenliğin temel kavramlarını**, varlık, tehdit, güvenlik açığı, risk ve kontrol terimlerini açıklayabileceksiniz.
- **NIST ekosistemindeki temel standartların ve yayınların** hangi amaçlarla kullanıldığını anlayabileceksiniz.
- **NIST SP 800-12, SP 800-53, SP 800-37 ve SP 800-171** yayınlarının temel kapsamlarını ayırt edebileceksiniz.
- **NIST'in risk temelli siber güvenlik yaklaşımını** açıklayabileceksiniz.
- **Varlıkları, tehditleri ve güvenlik açıklarını** belirleyerek temel risk değerlendirmelerine katkıda bulunabileceksiniz.
- **Olasılık, etki ve risk yanıtı** kavramlarını kurumsal güvenlik kararlarıyla ilişkilendirebileceksiniz.
- **NIST RMF'nin yedi aşamasını** ve bu aşamaların güvenlik kontrolleriyle ilişkisini açıklayabileceksiniz.
- **NIST SP 800-53 kontrol ailelerini** ve güvenlik kontrollerinin seçimi, uygulanması, değerlendirilmesi ve izlenmesi süreçlerini tanıyabileceksiniz.
- **İdari, teknik ve fiziksel güvenlik kontrollerini** birbirinden ayırt edebileceksiniz.
- **NIST CSF 2.0'ın altı fonksiyonunu** ve temel yapısını açıklayabileceksiniz.
- **Mevcut ve hedef profiller** ile **uygulama seviyelerinin** güvenlik iyileştirmelerindeki rolünü anlayabileceksiniz.
- **NIST SP 800-171** kapsamında hassas bilgilerin korunmasına yönelik temel gereklilikleri tanıyabileceksiniz.
- **Siber güvenlik farkındalığı ve çalışan sorumluluklarının** kurumsal güvenlik üzerindeki etkisini değerlendirebileceksiniz.
- **Olay yönetiminin hazırlık, tespit, analiz, sınırlandırma, müdahale ve kurtarma** aşamalarını açıklayabileceksiniz.
- **NIST kavramlarını örnek senaryolara uygulayarak** temel kurumsal siber güvenlik faaliyetlerini destekleyebileceksiniz.

## Eğitim İçeriği

### 1. Siber Güvenliğin Temelleri

# NIST Cybersecurity Foundation Eğitimi

Süre: **2 Gün**

BİLGİNÇ IT Academy
info@bilginc.com
bilginc.com

Bu bölümde, NIST rehberlerini anlamak için gerekli olan temel siber güvenlik kavramları açıklanır.

- **Siber güvenliğin temel terminolojisi ve ilkeleri**
- **Bilgi sistemleri (Information Systems)** kavramı
- **Varlıklar (Assets)** ve korunması gereken kaynaklar
- **Tehditler (Threats)** ve **güvenlik açıkları (Vulnerabilities)**
- **Risk** kavramı
- **Güvenlik kontrollerinin (Security Controls)** amacı
- **NIST ekosistemini anlamak için gerekli ortak terminolojinin** oluşturulması

## 2. NIST Siber Güvenlik Ekosistemi

Bu bölümde NIST tarafından yayımlanan standartların, çerçevelerin ve rehber dokümanların kullanım amaçları incelenir.

- **NIST standartlarına, çerçevelerine ve Özel Yayınlarına (Special Publications)** giriş
- **Kurumsal siber risk yönetimi rehberleri** ile **kontrol seçimi, uygulaması ve değerlendirmesine yönelik ayrıntılı yayınlar** arasındaki farkların açıklanması
- Temel NIST yayınlarının incelenmesi:
  - **NIST SP 800-12**
  - **NIST SP 800-53**
  - **NIST SP 800-37**
  - **NIST SP 800-171**
  - **NIST Cybersecurity Framework (CSF 2.0)**

## 3. Siber Güvenlik Risk Yönetimi

Bu bölümde NIST'in risk temelli siber güvenlik yaklaşımı ve risklerin değerlendirilmesine yönelik temel süreçler ele alınır.

- **Risk kavramlarına** ve NIST'in **risk temelli siber güvenlik yaklaşımına** giriş
- **Varlıkların, tehditlerin ve güvenlik açıklarının** belirlenmesi
- **Olasılık (Likelihood)** ve **etki (Impact)** kavramlarının anlaşılması
- **Risk düzeyinin** belirlenmesi
- Uygun **risk yanıtlarının (Risk Responses)** seçilmesi

BİLGİNÇ IT Academy

info@bilginc.com

bilginc.com


- **Risk farkındalığının** sürekli olarak korunması

## 4. NIST Risk Management Framework (RMF)

Bu bölümde **NIST Risk Yönetimi Çerçevesinin (RMF)** yaşam döngüsü ve güvenlik kontrolleriyle ilişkisi temel düzeyde incelenir.

**RMF'nin yedi aşaması:**

1. **Prepare (Hazırlık):** Risk yönetimi faaliyetleri için gerekli hazırlıkların yapılması
2. **Categorise (Kategorize Etme):** Sistemlerin ve bilgilerin sınıflandırılması
3. **Select (Seçim):** Uygun güvenlik kontrollerinin belirlenmesi
4. **Implement (Uygulama):** Seçilen kontrollerin hayata geçirilmesi
5. **Assess (Değerlendirme):** Kontrollerin değerlendirilmesi
6. **Authorise (Yetkilendirme):** Risklere ilişkin yetkilendirme kararlarının ele alınması
7. **Monitor (İzleme):** Güvenlik durumunun ve kontrollerin sürekli izlenmesi

## 5. NIST Güvenlik Kontrolleri

Bu bölüm, **NIST SP 800-53** kapsamında güvenlik kontrollerinin yapısına ve risk yönetimindeki kullanımına odaklanır.

- **NIST SP 800-53'ün amacı ve yapısı**
- **Kontrol ailelerinin (Control Families)** tanınması
- Güvenlik kontrollerinin **seçilmesi**
- Kontrollerin **uygulanması**
- Kontrol etkinliğinin **değerlendirilmesi**
- Kontrollerin **izlenmesi**
- **İdari (Administrative)**, **teknik (Technical)** ve **fiziksel (Physical)** kontroller arasındaki farklar
- Güvenlik kontrollerinin **risklerin ele alınmasını (Risk Treatment)** nasıl desteklediğinin açıklanması

## 6. NIST Cybersecurity Framework (CSF) 2.0

Bu bölümde **NIST CSF 2.0** çerçevesinin temel bileşenleri ve kurumsal güvenlik süreçlerinde kullanımı ele alınır.

**CSF 2.0'ın altı temel fonksiyonu:**

- **Govern (Yönet):** Siber güvenlik yönetişimi ve kurumsal sorumluluklar

BİLGİNÇ IT Academy

info@bilginc.com

bilginc.com


- **Identify (Belirle):** Varlıkların, risklerin ve ilgili unsurların tanımlanması
- **Protect (Koru):** Koruyucu güvenlik önlemlerinin uygulanması
- **Detect (Tespit Et):** Güvenlik olaylarının ve anormalliklerin belirlenmesi
- **Respond (Müdahale Et):** Tespit edilen olaylara yanıt verilmesi
- **Recover (Kurtar):** Olay sonrasında sistemlerin ve faaliyetlerin toparlanması

**Çerçevenin diğer bileşenleri:**

- **Functions (Fonksiyonlar)**
- **Categories (Kategoriler)**
- **Subcategories (Alt Kategoriler)**
- **Organisational Profiles (Kurumsal Profiller)**
- **Current Profile (Mevcut Profil)**
- **Target Profile (Hedef Profil)**
- **Implementation Tiers (Uygulama Seviyeleri)**

Ayrıca CSF'nin **siber güvenlik iyileştirmelerini planlama** ve **paydaşlar arasında ortak iletişim dili oluşturma** açısından sağladığı katkılar değerlendirilir.

## 7. Hassas Bilgilerin Korunması – NIST SP 800-171

Bu bölümde federal kurumlar dışındaki ortamlarda hassas bilgilerin korunmasına yönelik NIST yaklaşımı incelenir.

- **Controlled Unclassified Information (CUI)** kavramının açıklanması
- **Federal olmayan ortamlarda CUI bilgilerinin korunması**
- **Savunma ve kamu tedarik zincirleri** açısından NIST SP 800-171'in önemi
- **Bilgi gereklilikleri, güvenlik kontrolleri ve tedarikçi güvencesi** arasındaki ilişkinin değerlendirilmesi

## 8. Siber Güvenlik Farkındalığı ve Eğitim

Bu bölüm, NIST yaklaşımında insan faktörünün ve kurumsal güvenlik kültürünün önemini ele alır.

- Siber güvenlikte **insan faktörünün rolü**
- **Güvenlik farkındalığının** geliştirilmesi
- **Çalışanların güvenlik sorumlulukları**

BİLGİNÇ IT Academy

info@bilginc.com

bilginc.com


- **Kabul edilebilir davranışların** belirlenmesi
- Kuruluş genelinde **siber güvenlik yetkinliğinin** geliştirilmesi

## 9. Siber Güvenlik Olay Yönetimi

Bu bölümde siber güvenlik olaylarının yönetilmesine ilişkin temel süreçler açıklanır.

- **Olay yönetimine hazırlık (Preparation)**
- **Olayların tespit edilmesi (Detection)**
- **Olay analizi (Analysis)**
- **Olayın sınırlandırılması (Containment)**
- **Müdahale faaliyetleri (Response)**
- **Kurtarma ve toparlanma (Recovery)**
- Olay müdahalesinin **risk yönetimi, güvenlik kontrolleri, izleme ve kurumsal dayanıklılık** ile ilişkilendirilmesi

## 10. NIST Yaklaşımlarının Uygulamada Kullanılması

Bu bölümde NIST rehberlerinin örnek senaryolar üzerinden nasıl kullanılabileceği değerlendirilir.

- **NIST yayınlarının senaryo temelli uygulanması**
- Önemli **siber güvenlik risklerinin** belirlenmesi
- İlgili **CSF fonksiyonlarının** seçilmesi
- Uygun **güvenlik kontrol alanlarının** belirlenmesi
- **Siber güvenlik olaylarına yanıt** yaklaşımlarının değerlendirilmesi
- Aşağıdaki süreçler arasındaki ilişkinin pekiştirilmesi:

**Risk → Çerçeve → Kontroller → Uygulama → İzleme → Müdahale → İyileştirme**