alfatraining Beratung
beratung@alfatraining.de
0800 3456-500
Mo. - Fr. von 8 bis 17 Uhr kostenfrei aus allen Netzen.

Kursstart alle 4 Wochen

IT-Security-Beauftragte:r und -Manager:in

Der Kurs vermittelt unter anderem organisatorische und technische Sicherheitsmaßnahmen, physische Schutzmaßnahmen, rechtliche Rahmenbedingungen und den Einsatz von Künstlicher Intelligenz (KI). Du lernst zudem, wie man kritische Unternehmensinformationen effektiv vor Bedrohungen schützt.

Abschlussart
Zertifikat „IT-Security-Beauftragte:r mit TÜV Rheinland geprüfter Qualifikation"
Zertifikat „IT-Security-Manager:in mit TÜV Rheinland geprüfter Qualifikation"

Abschlussprüfung
Praxisbezogene Projektarbeiten mit Abschlusspräsentationen
IT-Security-Beauftragte:r mit TÜV Rheinland geprüfter Qualifikation
IT-Security-Manager:in mit TÜV Rheinland geprüfter Qualifikation

Dauer
8 Wochen

Unterrichtszeiten
Montag bis Freitag von 08:30 bis 15:35 Uhr
(in Wochen mit Feiertagen von 8:30 bis 17:10 Uhr)

Nächste Kursstarts
27.05.2024
24.06.2024
22.07.2024

LEHRGANGSZIEL

Als IT-Sicherheitsbeauftragte:r kennst du die wesentlichen Aspekte und Anforderungen der IT-Sicherheit: Datensicherheit und -schutz, physische IT-Sicherheit, Kryptographie, Netzsicherheit, PKI, Computersicherheit und organisatorische Sicherheit. Du weißt, die relevanten Standards nach ISO/IEC 27001 und des IT-Grundschutzes nach BSI in der Praxis umzusetzen.

Abschließend verstehst du, wie du als IT-Security-Manager:in kritische Unternehmensinformationen effektiv vor Bedrohungen und Risiken schützt.

ZIELGRUPPE

Dieser Lehrgang richtet sich an verantwortliche Personen aus den Bereichen IT-Sicherheit, Netz- und Systemadministration, IT-Organisation, IT-Beratung, Revision und Risikomanagement.

BERUFSAUSSICHTEN

Mit erfolgreichem Abschluss dieses Lehrganges werden dir Kompetenzen in der Planung, Umsetzung und Überwachung von IT-Sicherheitskonzepten nachgewiesen. Diese kannst du für Führungspositionen in der IT-Branche und auch branchenübergreifend für Unternehmen und Behörden mit hohem Aufkommen von persönlichen Daten einsetzen.

LEHRGANGSINHALTE

IT-SECURITY-BEAUFTRAGTE:R MIT TÜV RHEINLAND GEPRÜFTER QUALIFIKATION

Aufbau und Kernprozesse der IT-Sicherheit (ca. 2 Tage)
Struktur der IT-Security in Unternehmen und deren wirtschaftliche Bedeutung
Beteiligte Personen, Funktionen und Kommunikationswege innerhalb des IT-Netzwerks
Grundlegende Vorschriften, rechtliche Grundsätze, Normen

Physische Sicherheit im IT-Umfeld (ca. 2 Tage)
Klassifizierung der physikalischen Sicherheit
Einführung in die physischen Gefahrennormen
Sicherheitsmaßnahmen für die IT-Infrastruktur
Kontroll- und Alarmierungsmechanismen

Künstliche Intelligenz (KI) im Arbeitsprozess
Vorstellung von konkreten KI-Technologien im beruflichen Umfeld
Anwendungsmöglichkeiten und Praxis-Übungen

Identity- und Access-Management (ca. 2 Tage)
Grundlagen des Access-Managements
Unterscheidung und Spezifizierung der Zutritts-, Zugangs- und Zugriffkontrollen in einem Unternehmen sowie deren Umsetzung
Konzeption und Kontrolle im Accessmanagement
Revisionssichere Archivierung
Identitätsprüfung und Rechtezuweisung
Schutzmechanismen für die IT-Infrastruktur

Bedrohungsszenarien und Konsequenzen für die Umsetzung im Unternehmen (ca. 3 Tage)
DLP – die Bedeutung von Data Loss Prevention und Data Leakage Prevention in der IT-Security
Maßnahmen der Data Loss Prevention und Data Leakage Prevention
Klassifizierung und Schutz vor Schadprogrammen
IOT (Internet Of Things) und Industrie 4.0 – mögliche Bedrohungsszenarien

Network-Security (ca. 2 Tage)
Besondere Maßnahmen für den Schutz des Netzwerkes
Datenschutzanforderungen an Mailserver
Verwaltung und Sicherheit bei Cloud-Nutzung
Prüfung der Systembestandteile und -anwendungen gegenüber unautorisierten Personen/Programmen/Fernzugriffen

Analyse und Realisierung eines IT-Sicherheitssystems für Unternehmen (ca. 2 Tage)

Grundlagen des Informationssicherheitsstandards nach ISO/IEC 27001:2022 sowie des Bundesamts für Sicherheit in der Informationstechnik (BSI) (ca. 2 Tage)

Struktur und Umsetzung des Notfallmanagements nach BSI-Standard 100-4 und 200-4 (BCM) (ca. 1 Tag)

IT-Sicherheit im Unternehmen – Trainings und Sensibilisierung für Mitarbeiter:innen (ca. 1 Tag)

Projektarbeit, Zertifizierungsvorbereitung und Zertifizierungsprüfung „IT-Security-Beauftragte:r mit TÜV Rheinland geprüfter Qualifikation" (ca. 3 Tage)

IT-SECURITY-MANAGER:IN MIT TÜV RHEINLAND GEPRÜFTER QUALIFIKATION

Unternehmensstrukturen und Steuerung der IT-Security (ca. 5 Tage)
Stellenwert der IT-Security in der Unternehmensstruktur heutiger Firmen
Rechtliche Grundlagen und deren Befolgung in der IT-Governance
Maßgebende Kennzahlen und Kontrollmechanismen im Information-Security-Management
Verantwortungsbereiche und Funktionen beteiligter Personen/Abteilungen
Definition der Richtlinien und Anwendungsbereiche eines ISMS (Information Security Management System)

Künstliche Intelligenz (KI) im Arbeitsprozess
Vorstellung von konkreten KI-Technologien im beruflichen Umfeld
Anwendungsmöglichkeiten und Praxis-Übungen

Standards und Grundsätze in der IT-Sicherheit (ca. 2 Tage)

Aufbau und Leitfaden eines ISMS nach DIN ISO/IEC 27001, 27002:2022 (ca. 3 Tage)
Bedeutung und Anwendungsübersicht der Norm
Anforderungen der Norm an ein dokumentiertes ISMS und der Implementierung von geeigneten Sicherheitsmechanismen
Umsetzung, Überwachung und fortdauernde Verbesserungen
Bedeutung der Norm für den Schutz der Assets in einem Unternehmen
IT-Risk Management nach ISO/IEC 27005:2022, IT-Hauptrisiken
Evaluierung der Bedrohungen und Schwächen in einem ISMS und deren Auswirkungen

Betriebliche Umsetzung eines ISMS
Einsatz eines aktuellen ISMS-Tools (ca. 4 Tage)
Projektierung und Umsetzung auf Basis des OpenSource ISMS-Werkzeuges „verinice“
Analyse der bestehenden Risiken sowie Planung der entsprechenden Risikobehandlung
Überprüfung/Testen des entwickelten Risikobehandlungskonzeptes
Kontrolle der Wirksamkeit der vorläufig implementierten Maßnahme
Implementierung des entwickelten Systems und kontinuierliche Überprüfung
Statement of Applicability
Methoden zur Sensibilisierung und Schulung im Unternehmen
Management von IS Vorfällen (Information Security Incident Management)

Projektmanagement (ca. 1 Tag)
Praktische Anwendung von Projektmanagementmethoden zur Initiierung, Definition, Planung, Controlling und Abschluss
Anwendung von Softwaretools, Kommunikation und Führungswerkzeugen

Sicherstellung der korrekten Umsetzung der Norm und Standards Audits/Zertifizierung (ca. 2 Tage)
Dokumentation und Berichtswesen in einem ISMS
Interne Audits
Managementbewertungen
Zertifizierung des ISMS

Projektarbeit, Zertifizierungsvorbereitung und Zertifizierungsprüfung „IT-Security-Manager:in mit TÜV Rheinland geprüfter Qualifikation“ (ca. 3 Tage)

UNTERRICHTSKONZEPT

Didaktisches Konzept
Deine Dozierenden sind sowohl fachlich als auch didaktisch hoch qualifiziert und werden dich vom ersten bis zum letzten Tag unterrichten (kein Selbstlernsystem).
Du lernst in effektiven Kleingruppen. Die Kurse bestehen in der Regel aus 6 bis 25 Teilnehmenden. Der allgemeine Unterricht wird in allen Kursmodulen durch zahlreiche praxisbezogene Übungen ergänzt. Die Übungsphase ist ein wichtiger Bestandteil des Unterrichts, denn in dieser Zeit verarbeitest du das neu Erlernte und erlangst Sicherheit und Routine in der Anwendung. Im letzten Abschnitt des Lehrgangs findet eine Projektarbeit, eine Fallstudie oder eine Abschlussprüfung statt.

Virtueller Klassenraum alfaview®
Der Unterricht findet über die moderne Videotechnik alfaview® statt - entweder bequem von zu Hause oder bei uns im Bildungszentrum. Über alfaview® kann sich der gesamte Kurs face-to-face sehen, in lippensynchroner Sprachqualität miteinander kommunizieren und an gemeinsamen Projekten arbeiten. Du kannst selbstverständlich auch deine zugeschalteten Trainer:innen jederzeit live sehen, mit diesen sprechen und du wirst während der gesamten Kursdauer von deinen Dozierenden in Echtzeit unterrichtet. Der Unterricht ist kein E-Learning, sondern echter Live-Präsenzunterricht über Videotechnik.

FÖRDERMÖGLICHKEITEN

Die Lehrgänge bei alfatraining werden von der Agentur für Arbeit gefördert und sind nach der Zulassungsverordnung AZAV zertifiziert. Bei der Einreichung eines Bildungsgutscheines oder eines Aktivierungs- und Vermittlungsgutscheines werden in der Regel die gesamten Lehrgangskosten von deiner Förderstelle übernommen.
Eine Förderung ist auch über den Europäischen Sozialfonds (ESF), die Deutsche Rentenversicherung (DRV) oder über regionale Förderprogramme möglich. Als Zeitsoldat:in besteht die Möglichkeit, Weiterbildungen über den Berufsförderungsdienst (BFD) zu besuchen. Auch Firmen können ihre

Mitarbeiter:innen über eine Förderung der Agentur für Arbeit (Qualifizierungschancengesetz) qualifizieren lassen.

ⓘ Änderungen möglich. Die Lehrgangsinhalte werden regelmäßig aktualisiert. Die aktuellen Lehrgangsinhalte findest Du immer unter www.alfatraining.de.