INEFOP en Coursera: Programa 3: Certificaciones Profesionales de IBM - Analista de ciberseguridad					
Nombre del curso	**Descripcion del curso**	**Idioma del curso**	**Cursos con subtitulos**	**Institución**	**Nivel de dificultad**
Introduction to Cybersecurity Tools & Cyber Attacks	This course gives you the background needed to understand basic Cybersecurity. You will learn the history of Cybersecurity, types and motives of cyber attacks to further your knowledge of current threats to organizations and individuals. Key terminology, basic system concepts and tools will be examined as an introduction to the Cybersecurity field.\n\nYou will learn about critical thinking and its importance to anyone looking to pursue a career in Cybersecurity.\n\nFinally, you will begin to learn about organizations and resources to further research cybersecurity issues in the Modern era.\n\nThis course is intended for anyone who wants to gain a basic understanding of Cybersecurity or as the first course in a series of courses to acquire the skills to work in the Cybersecurity field as a Jr Cybersecurity Analyst.\n\nThe completion of this course also makes you eligible to earn the Introduction to Cybersecurity Tools & Cyber Attacks IBM digital badge. More information about the badge can be found https://www.youracclaim.com/org/ibm/badge/introduction-to-cybersecurity-tools-cyber-attacks	Inglés	SI	IBM	Principiante
Cybersecurity Roles, Processes & Operating System Security	This course gives you the background needed to understand basic Cybersecurity around people. process and technology. You will learn:\n\n•\t Understand the key cybersecurity roles within an Organization. \n•\t List key cybersecurity processes and an example of each process.\n•\t Describe the architecture, file systems, and basic commands for multiple operating systems including Windows, Mac/OS, Linux and Mobile.\n•\t Understand the concept of Virtualization as it relates to cybersecurity \n\nFinally, you will begin to learn about organizations and resources to further research cybersecurity issues in the Modern era.\n\nThis course is intended for anyone who wants to gain a basic understanding of Cybersecurity or as the second course in a series of courses to acquire the skills to work in the Cybersecurity field as a Jr Cybersecurity Analyst.\n\nThe completion of this course also makes you eligible to earn the Cybersecurity Roles, Processes & Operating System Security IBM digital badge. More information about the badge can be found here: https://www.youracclaim.com/org/ibm/badge/cybersecurity-roles-processes-operating-system-security	Inglés	SI	IBM	Principiante

Cybersecurity Compliance Framework & System Administration	This course gives you the background needed to understand the key cybersecurity compliance and industry standards. This knowledge will be important for you to learn no matter what cybersecurity role you would like to acquire or have within an organization.\n\n You will learn the basic commands for user and server administration as it relates to security. You will need this skill to be able to understand vulnerabilities within your organizations operating systems.\n\nYou will learn the concepts of endpoint security and patch management. Both of these topics are important to keep systems current to avoid cybersecurity incidents against an organization.\n\nFinally you will learn in depth skills around cryptography and encryption to understand how these concepts affect software within a company. \n\nThis course is intended for anyone who wants to gain a basic understanding of Security Frameworks, Compliance, endpoint management, encryption or cryptography or as the third course in a series of courses to gain the skill as a Jr Cybersecurity analyst.	Inglés	SI	IBM	Principiante
Network Security & Database Vulnerabilities	This course gives you the background needed to understand basic network security. You will learn the about Local Area Networks, TCP/IP, the OSI Framework and routing basics. You will learn how networking affects security systems within an organization. You will learn the network components that guard an organization from cybersecurity attacks.\n\nIn addition to networking, you will learn about database vulnerabilities and the tools/knowledge needed to research a database vulnerability for a variety of databases including SQL Injection, Oracle, Mongo and Couch. \n\nYou will learn about various security breach types associated with databases and organizations that define standards and provide tools for cybersecurity professionals.\n\nThis course is intended for anyone who wants to gain a basic understanding of Network Security/Database Vulnerabilities or as the fourth course in a series of courses to acquire the skills to work in the Cybersecurity field as a Jr Cybersecurity Analyst.	Inglés	SI	IBM	Principiante
Penetration Testing, Incident Response and Forensics	This course gives you the background needed to gain Cybersecurity skills as part of the Cybersecurity Security Analyst Professional Certificate program. \n\nYou will learn about the different phases of penetration testing, how to gather data for your penetration test and popular penetration testing tools. Furthermore, you will learn the phases of an incident response, important documentation to collect, and the components of an incident response policy and team. Finally, you will learn key steps in the forensic process and important data to collect. \n\nThis course also gives you a first look at scripting and the importance to a system analyst.\n\nThis course is intended for anyone who wants to gain a basic understanding of Cybersecurity or as the fifth course in a series of courses to acquire the skills to work in the Cybersecurity field as a Cybersecurity Analyst.\n\nThe completion of this course also makes you eligible to earn the Penetration Testing, Incident Response and Forensics IBM digital badge. More information about the badge can be found https://www.youracclaim.com/org/ibm/badge/penetration-testing-incident-response-and-forensics.\n\n\nIn this course you will learn to:\n•\tDescribe penetration testing tools and the benefits to an organization\n•\tDescribe a deep dive into incident response techniques and tools\n•\tDescribe digital forensics and digital evidence.\n•\tDiscuss the power of scripting.	Inglés	SI	IBM	Principiante

Cybersecurity Capstone: Breach Response Case Studies	This course gives you the background needed to gain Cybersecurity skills as part of the Cybersecurity Security Analyst Professional Certificate program. \n\nYou will explore incident response methodologies and security models. You will learn to recognize and categorize key types of vulnerabilities and associated attacks against today's organizations. You will explore in depth several past and recent breaches to learn how they were detected and what was done or could have been done to reduce the threat risk to the organization.\nFinally, you will explore the costs of data breaches through research studies and well known breaches.\n\nThis course requires you to select and research a cybersecurity breach in the news today and apply your knowledge and skills from this course and previous cybersecurity courses to analyze the type of attack, attack timeline, vulnerable systems, and any missed opportunities. This project will be graded by your peers in the course.\n\nThis course is intended for anyone who wants to gain a basic understanding of Cybersecurity or as the seventh and final course in a series of courses to acquire the skills to work in the Cybersecurity field as a Cybersecurity Analyst.\n\nThe completion of this course also makes you eligible to earn the Cybersecurity Capstone: Breach Response Case Studies IBM digital badge. More information about the badge can be found https://www.youracclaim.com/org/ibm/badge/cybersecurity-breach-case-studies .\n\nIn this course, you will learn to:\n\n•\tApply incident response methodologies.\n•\tResearch and describe a watering hole attack.\n•\tResearch and describe ransomware threats and the consequences to organization.\n•\tResearch and describe 3rd party breaches and how they affect an organization.\n•\tResearch and describe the effects of a phishing attack.\n•\tResearch and describe a point of sale attack and approximate cost of data breaches.\n•\tPerform a case study on a current cyber attack and breach.	Inglés	SI	IBM	Principiante
IBM Cybersecurity Analyst Assessment	A growing number of exciting, well-paying jobs in today's security industry do not require a college degree. This is the final course required to assess your acquired knowledge and skills from from the previous two specializations, IT Fundamentals of Cybersecurity and Security Analyst Fundamentals, to become job-ready for a cybersecurity analyst role. \n\nYou will be expected to pass a final assessment quiz for each of the seven (7) prior courses within the IBM Cybersecurity Analyst Professional Certificate.\n\nUpon successful completion of the quizzes, you will acquire the IBM Cybersecurity Analyst Professional Certificate.	Inglés	NO	IBM	Avanzado
Cyber Threat Intelligence	This course gives you the background needed to gain Cybersecurity skills as part of the Cybersecurity Security Analyst Professional Certificate program. \n\nYou will understand network defensive tactics, define network access control and use network monitoring tools. You will understand data protection risks and explore mobile endpoint protection. Finally you will recognize various scanning technologies, application security vulnerabilities and threat intelligence platforms.\n\nThis course also gives you hands on access to cybersecurity tools important to a system analyst.\n\nThis course is intended for anyone who wants to gain a basic understanding of Cybersecurity or as the sixth course in a series of courses to acquire the skills to work in the Cybersecurity field as a Cybersecurity Analyst.\n\nThe completion of this course also makes you eligible to earn the Cyber Threat Intelligence IBM digital badge. More information about the badge can be found https://www.youracclaim.com/org/ibm/badge/cyber-threat-intelligence.\n\nIn this course, you will learn to:\n\n•\tDescribe examples of network defensive tactics.\n•\tDiscuss data loss prevention and endpoint protection concepts and tools. \n•\tExplore a data loss prevention tool and learn how to classify data in your database environment. \n•\tDescribe security vulnerability scanning technologies and tools.\n•\tRecognize application security threats and common vulnerabilities.\n•\tIdentify the key concepts around threat intelligence.\n•\tExplore a SIEM product and review suspicious alerts and how to take action.	Inglés	SI	IBM	Avanzado