CertiProf Lead Cybersecurity Professional Certificate (LCSPC)

Sample Exam (V082019)

1. It is not a NIST CSF objective:

a) Assist critical infrastructure managers and operators to identify, inventory and manage IT risks.
b) Establish a different language for managing Cybersecurity risks.
c) Establish criteria for the definition of metrics to control implementation performance.
d) None of the above.

2. NIST CSF Framework Profiles:

a) Present industry standards, guidelines, and practices in a manner that allows communication of Cybersecurity activities and results.
b) Provide a context for how an organization views the risk of Cybersecurity.
c) Represents the results based on business needs that an organization has selected from the Categories and Subcategories.
d) None of the above.

3. It is not a function of the NIST CSF Core Framework:

a) Detect (DE).
b) Analyze (AN).
c) Identify (ID).
d) None of the above.

4. The Retrieve function allows:

a) To develop and implement appropriate activities to maintain resilience plans.
b) To develop and implement appropriate activities to identify the occurrence of a Cybersecurity event.
c) To develop and implement appropriate safeguards to ensure the provision of critical infrastructure services.
d) None of the above.

5. The subcategories are:

   a) Extension of Cybersecurity functions.
   b) Cybersecurity Controls.
   c) Specific sections of rules.
   d) None of the above.

6. The NIST Framework consists of 5 simultaneous and continuous functions:

   a) False.
   b) True.

7. The INFORMED RISK Implementation Level must comply with the following in the risk management process:

   a) Risk management practices are approved by management but cannot be established as organization-wide policies.
   b) The risk management practices of the organization are formally approved and expressed as policies.
   c) The organization adapts its Cybersecurity practices based on lessons learned and predictive indicators.
   d) None of the above.

8. Do the 5 continuous functions of the NIST CSF give rise to the life cycle of Cybersecurity?

   a) True.
   b) False.
   c) It depends on the interested parties.
   d) None of the above.

9. The activity «create a current CSF profile» indicates the following:

   a) The organization creates an objective profile that focuses on evaluating the categories and subcategories of the framework that describe the organization's desired Cybersecurity outcomes.
   b) The organization develops a current profile indicating the category and subcategory results of the core Framework that are currently being achieved.
   c) This assessment could be guided by the organization's overall risk management process or previous risk assessment activities.

10. The Identify function allows:

a) To develop and implement appropriate activities to maintain resilience plans.
b) To develop organizational understanding to manage Cybersecurity risk to systems, assets, data and capabilities.
c) To develop and implement appropriate safeguards to ensure the provision of critical infrastructure services.
d) None of the above.

11. The statement «The Framework provides a common language for communicating requirements among interdependent stakeholders responsible for the delivery of essential critical infrastructure services,» is:

a) True.
b) False.
c) Depends on the parties concerned.
d) None of the above.

12. The purpose and scope of ISO/IEC 27032 is:

a) To provide guidance to improve the state of Cybersecurity, highlighting unique aspects of such activity and its dependence on other areas of security.
b) To apply as a reference framework for information security in Latin American member countries.
c) To develop and implement appropriate activities to maintain Cyber resilience plans.
d) None of the above.

13. According to ISO/IEC 27032, one of the following areas is not related to Cybersecurity.

a) Information Security.
b) Internet security.
c) HR Security.
d) None of the above.

14. Among the interested parties within cyberspace, we have suppliers, which include:

a) Server providers.
b) Application providers.
c) Remote access providers.
d) None of the above.

15. Cyberspace assets maintain a category that is Personal Assets, which include:

a) Laptop of the entity.
b) Intellectual property.
c) Virtual currency.
d) None of the above.

16. One of the following is not a Threat to Personal Assets.

a) Improper access and exploitation.
b) Theft of the person's money and fraud.
c) Leakage or theft of personal information.
d) None of the above.

17. One of the following is not a Role of Cybersecurity stakeholders.

a) Roles of organizations.
b) Consumer roles.
c) Roles of partners.
d) None of the above.

18. The Guidelines for Organizations and Service Providers indicate that it is necessary to:

a) Manage the risk of information security in the business, among others.
b) They should guide consumers on how to stay safe online, among others.
c) How they could positively influence the state of Cybersecurity, among others.
d) None of the above.

19. According to ISO/IEC 27032, Cybersecurity controls maintain the following categories:

a) Software Level Controls, Service Protection, End User Controls, and Social Engineering Attack Controls.
b) Application Level Controls, Service Protection, End User Controls and Reverse Engineering Attack Controls.
c) Application Level Controls, Server Protection, End User Controls, and Social Engineering Attack Controls.
d) None of the above.

20. The Framework for Information Exchange and Coordination, include:

a) Strategic partners.
b) People and Organizations.
c) Learning techniques.
d) None of the above.

21. The controls of ISO/IEC 27032 can be included, on a supplementary basis with ISO 27001, in:

a) SGSI policy.
b) SGSI scope.
c) The Statement of Applicability- SoA.
d) None of the above.

22. The NIST Framework includes other standards as normative reference controls, such as:

a) ISO/IEC 27001, NIST SP 800-82, ISA 62443.
b) CIS CSC 7.1, COBIT 2019, ISO 31000.
c) ISO/IEC 27032, ISO/IEC 27002, ISO 38500.
d) All of the above.
e) None of the above.

23. The NIST Framework consists of 5 simultaneous and continuous functions:

a) Intensify, Protect, Detect, Reply and Recover.
b) Identify, Protect, Detect, Attack and Recover.
c) Implement, Protect, Defend, Resist, Resilience.
d) Identify, Protect, Detect, Reply and Recover.
e) None of the above.

24. The difference between Cybersecurity and Information Security: *Information Security deals with information regardless of its format; and Cybersecurity refers to the protection of digital assets.*

a) False.
b) True.

25. For Cybersecurity risk management, which methodology can you use as a reference?

a) ISO 31000.
b) ISO/IEC 27005.
c) Cobit for Risk.
d) All of the above.
e) None of the above.

26. It is defined as a type of malicious program that seizes information, restricting access to it and requesting the payment of a ransom in exchange for removing this restriction.

a) Cryptojacking.
b) Botnet.
c) Ransomware.
d) Shadow IT.
e) Spear Phishing.

27. A process that identifies the threats and dangers that exist for an organization is:

a) Disaster recovery.
b) Business continuity.
c) Cybersecurity Risk Management.
d) Information security.
e) None of the above

28. The most effective way to mitigate the threat of social engineering is with the help of:

a) Purchase state-of-the-art information security technologies.
b) Campaign on Social Engineering as part of Information Security.
c) Implement a permanent education and awareness program on Cybersecurity.
d) B and C are valid.
e) None of the above.

29. Roles and responsibilities within the NIST Cyber security Framework are defined in controls ID.AM-6 and PR-AT-3.

a) True.
b) False.

30. To measure the effectiveness of the Cybersecurity Program one should:

a) Define indicators using the SMART methodology.
b) Purchase an automated tool.
c) None of the above.
d) All of the above.

Answers

1.	B
2.	C
3.	B
4.	A
5.	B
6.	B
7.	A
8.	A
9.	B
10.	B
11.	A
12.	A
13.	C
14.	B
15.	C
16.	A
17.	C
18.	A
19.	C
20.	B
21.	C
22.	A
23.	D
24.	B
25.	D
26.	C
27.	C
28.	D
29.	A
30.	A