PROCEDURA DI SELEZIONE PUBBLICA PER ESAMI PER IL RECLUTAMENTO DI N. Prot n.0125825 del 15/05/2026 UNITÀ DI PERSONALE A TEMPO INDETERMINATO DI AREA DEI FUNZIONARI, A TEMPO INDETERMINATO (36 ORE SETTIMANALI), PRESSO L'AREA SERVIZI ICT DEL POLITECNICO DI MILANO INDETTA CON D.D. N. 9723/2026 DEL 15.05.2026, 2026 PTA_TI_D_DIRGEN_6

Traccia 1

1. Con riferimento ad OWASP Top Ten Web Application Security Risks, spiegare in dettaglio le tipologie ed il funzionamento degli attacchi di tipo Cross-site scripting (XSS). Elencare le possibili contromisure.

2. Spiegare il concetto di Buffer Overflow, proporre un esempio di codice vulnerabile in un linguaggio di programmazione a propria scelta e indicare una possibile mitigazione.

3. Si consideri il processo di Vulnerability Assessment. Illustrare le fasi del processo e descrivere i concetti di Common Vulnerability Scoring System (CVSS) e di Common Vulnerabilities and Exposures (CVE) e come questi possono essere utili nella prioritizzazione delle attività di remediation.

PROCEDURA DI SELEZIONE PUBBLICA PER ESAMI PER IL RECLUTAMENTO DI N. Prot n.0125825 del 15/05/2026 UNITÀ DI PERSONALE A TEMPO INDETERMINATO DI AREA DEI FUNZIONARI, A TEMPO INDETERMINATO (36 ORE SETTIMANALI), PRESSO L'AREA SERVIZI ICT DEL POLITECNICO DI MILANO INDETTA CON D.D. N. 9723/2026 DEL 15.05.2026, 2026 PTA_TI_D_DIRGEN_6

Traccia 2

1. Con riferimento ad OWASP Top Ten Web Application Security Risks, spiegare in dettaglio le tipologie ed il funzionamento degli attacchi di tipo SQL-Injection. Elencare le possibili contromisure.

2. Spiegare il concetto di Confused Deputy, descrivere un esempio di occorrenza. Elencare le possibili contromisure.

3. Si consideri il processo di Penetration Testing. Illustrare le fasi del processo e le differenze tra gli approcci White-Box, Black-box e Grey-box

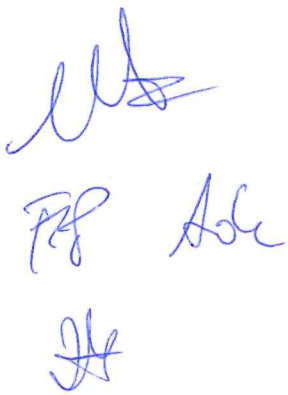
PROCEDURA DI SELEZIONE PUBBLICA PER ESAMI PER IL RECLUTAMENTO DI N. Prot n.0125825 del 15/05/2026 UNITÀ DI PERSONALE A TEMPO INDETERMINATO DI AREA DEI FUNZIONARI, A TEMPO INDETERMINATO (36 ORE SETTIMANALI), PRESSO L'AREA SERVIZI ICT DEL POLITECNICO DI MILANO INDETTA CON D.D. N. 9723/2026 DEL 15.05.2026, 2026 PTA_TI_D_DIRGEN_6

Traccia 3

1. Con riferimento ad OWASP Top Ten Web Application Security Risks, spiegare in dettaglio alcuni possibili attacchi per l'esfiltrazione di un cookie di sessione. Elencare i possibili attributi di sicurezza dei cookie stessi per mitigare il rischio.

2. Spiegare il concetto di Dangling Pointer, proporre un esempio di codice vulnerabile in un linguaggio di programmazione a propria scelta e indicare una possibile mitigazione.

3. Si consideri il processo di Log Management. Illustrare quali sono le principali categorie di log di interesse per un Security Operation Center in ambito universitario e descrivere il concetto di SIEM.
   Si consideri l'evento "Un server web riporta ripetuti tentativi di accesso falliti provenienti dallo stesso indirizzo IP": descrivere quali informazioni cercare nei log e come determinare se si tratta di un attacco.



PROCEDURA DI SELEZIONE PUBBLICA PER ESAMI PER IL RECLUTAMENTO DI N. 1 UNITÀ DI PERSONALE A TEMPO INDETERMINATO DI AREA DEI FUNZIONARI(36 ORE SETTIMANALI), PRESSO L'AREA SERVIZI ICT DEL POLITECNICO DI MILANO INDETTA CON D.D. N. 9723/2026 PROT. N.0125825 DEL 15/05/2026, 2026 PTA_TI_D_DIRGEN_6

Traccia Orale 1

a) Descrivere il Mitre Attack Framework e descrivere come lo si applicherebbe al seguente incidente: "Active Directory Domain Controller full compromise".

b) Descrivere il funzionamento di un Web Application Firewall (WAF), soffermandosi sulle principali categorie di attacco applicabili e tecniche di aggiramento delle protezioni stesse

c) Si descriva il concetto di "tabella pivot" all'interno del pacchetto Office

d) Tradurre in italiano il seguente testo:

Since the entry into force of Directive (EU) 2016/1148, significant progress has been made in increasing the Union's level of cyber resilience. The review of that Directive has shown that it has served as a catalyst for the institutional and regulatory approach to cybersecurity in the Union, paving the way for a significant change in mind-set. That Directive has ensured the completion of national frameworks on the security of network and information systems by establishing national strategies on security of network and information systems and establishing national capabilities and by implementing regulatory measures covering essential infrastructures and entities identified by each Member State. Directive (EU) 2016/1148 has also contributed to cooperation at Union level through the establishment of the Cooperation Group and the network of national computer security incident response teams. Notwithstanding those achievements, the review of Directive (EU) 2016/1148 has revealed inherent shortcomings that prevent it from addressing effectively current and emerging cybersecurity challenges.

PROCEDURA DI SELEZIONE PUBBLICA PER ESAMI PER IL RECLUTAMENTO DI N. 1 UNITÀ DI PERSONALE A TEMPO INDETERMINATO DI AREA DEI FUNZIONARI(36 ORE SETTIMANALI), PRESSO L'AREA SERVIZI ICT DEL POLITECNICO DI MILANO INDETTA CON D.D. N. 9723/2026 PROT. N.0125825 DEL 15/05/2026, 2026 PTA_TI_D_DIRGEN_6

Traccia Orale 2

a) Descrivere il processo di cyber incident response

b) Descrivere il funzionamento di un Intrusion Prevention System (IPS), soffermandosi sulle principali categorie di attacco applicabili e tecniche di aggiramento delle protezioni stesse

c) Si descriva il concetto di "formattazione condizionale" all'interno del pacchetto Office

d) Tradurre in italiano il seguente testo:

This document has been prepared to provide requirements for establishing, implementing, maintaining and continually improving an information security management system. The adoption of an information security management system is a strategic decision for an organization. The establishment and implementation of an organization's information security management system is influenced by the organization's needs and objectives, security requirements, the organizational processes used and the size and structure of the organization. All of these influencing factors are expected to change over time.
The information security management system preserves the confidentiality, integrity and availability of information by applying a risk management process and gives confidence to interested parties that risks are adequately managed.
It is important that the information security management system is part of and integrated with the organization's processes and overall management structure and that information security is considered in the design of processes, information systems, and controls. It is expected that an information security management system implementation will be scaled in accordance with the needs of the organization.

PROCEDURA DI SELEZIONE PUBBLICA PER ESAMI PER IL RECLUTAMENTO DI N. 1 UNITÀ DI PERSONALE A TEMPO INDETERMINATO DI AREA DEI FUNZIONARI(36 ORE SETTIMANALI), PRESSO L'AREA SERVIZI ICT DEL POLITECNICO DI MILANO INDETTA CON D.D. N. 9723/2026 PROT. N.0125825 DEL 15/05/2026, 2026 PTA_TI_D_DIRGEN_6

Traccia Orale 3

a) Descrivere il funzionamento di un sistema di Endpoint Detection and Response (EDR), soffermandosi sulle principali categorie di attacco applicabili e tecniche di aggiramento delle protezioni stesse

b) Descrivere il concetto di attacco Distributed Denial of Service DDoS, evidenziando quali protocolli sono tipicamente utilizzati per effettuare questo tipo di attacco. Soffermarsi su possibili impatti e mitigazioni in ambiente cloud.

c) Si descriva il concetto di "stampa unione" all'interno del pacchetto Office

d) Tradurre in italiano il seguente testo:

This publication provides results-driven guidance for those who are interested in establishing a computer security incident response team (CSIRT) or security operations centre (SOC), and guidance on possible improvements for different types of CSIRTs and SOCs that exist currently.

The content of this report is based on an analysis of current publications on the establishment of CSIRTs (the analysis is summarised in Annex B); a field questionnaire (Annex A), which was completed by 40 CSIRTs and SOCs; and the authors' experiences in establishing and improving CSIRTs as part of numerous projects carried out in Europe, Asia, Africa and South

America. A results-driven approach is taken throughout the publication to provide guidance on the different stages involved in the establishment of a CSIRT or SOC organisation:

- Assessment for readiness
- Design
- Implementation
- Operations
- Improvement.