# CISP练习习题整理

## 一、信息安全管理

### 题目1

小陈在某电器城购买了一台冰箱，并留下了个人姓名、电话和电子邮件地址等信息，第二天他收到了一封来自电器城提示他中奖的邮件，查看该邮件后他按照提示操作缴纳中奖税款后并没有得到中奖奖金，再打电话询问电器城才得知电器城并没有中奖的活动。在此案例中，下面描述错误的是()

A. 小陈应当注意保护自己的隐私，没有必要告诉别人的信息不要登记和公布给别人

B. 小陈钱被编走了，这类网络犯罪案件也应该向公安局报案

C. 邮件服务运营商通过技术手段，可以在一定程度上阻止此类钓鱼邮件和哄骗邮件

D. 小陈应当向电器城索赔，追回损失

**答案：D**

**解析**：电器城并未举办中奖活动，小陈的个人信息可能被第三方非法获取并用于诈骗，因此电器城不承担赔偿责任。

### 题目2

在 GB/T 1836《信息技术安全性评估准则》中，有关保护轮廓(Protection Profile, PP)和安全目标(Security Target，ST)，错误的是：

A. PP 是描述一类产品或系统的安全要求

B. PP 描述的安全要求与具体实现无关

C. 两份不同的 ST 不可能满足同一份 PP 的要求

D. ST 与具体的实现有关

**答案：C**

**解析**：保护轮廓（PP）是对一类产品或系统的通用安全要求，而安全目标（ST）是针对具体产品或系统的安全要求。不同的ST可以满足同一份PP的要求，只要它们都覆盖了PP中规定的安全需求。

## 二、网络安全技术

### 题目3

下面哪一项不是虚拟专用网络(VPN)协议标准：

A. 第二层隧道协议(L2TP)

B. Internet 安全性(IPSEC)

C. 终端访问控制器访问控制系统

D. 点对点隧道协议(PPTP)

**答案：C**

**解析**：终端访问控制器访问控制系统（TACACS）是一种远程认证协议，不属于VPN协议。常见的VPN协议包括L2TP、IPSec和PPTP。

### 题目4

以下有关服务协议的介绍哪一个是错误的?

A. SMTP 简单邮件传输协议使用 TCP 协议，端口号是 25

B. FTP 文件传输协议(数据连接服务)使用 TCP，端口号是 20

C. DNS 域名解析服务协议使用 TCP 协议，端口号 53

D. TFTP 简单文件传输协议使用 UDP 协议，端口号 69

**答案：C**

**解析**：DNS协议通常使用UDP端口53进行域名解析，仅在进行区域传输时使用TCP端口53。

## 三、信息安全基础

### 题目5

一个较为可靠的鉴别系统一般是由以下哪几部份组成：

A. 验证者、被验证者和中间人

B. 验证者、被验证者和可信赖方

C. 验证者和被验证者

D. 验证者、被验证者和鉴别方

**答案：B**

**解析**：可靠的鉴别系统通常包括验证者（发起鉴别请求）、被验证者（接受鉴别）和可信赖方（如CA机构，提供证书验证），以确保鉴别过程的安全性和可靠性。

## 五、AI防御与新兴技术安全

### 题目16

以下关于AI系统内生风险的描述中，错误的是：

A. 对抗性样本攻击属于模型层风险

B. 训练数据污染可能导致模型决策偏差

C. 模型逃逸攻击可绕过内容审核机制

D. 资源耗尽攻击属于数据层风险

**答案：D**

**解析**：资源耗尽攻击属于AI系统层风险（如恶意触发大模型算力过载），而非数据层风险。数据层风险主要包括训练数据泄露、隐私推理等，因此D选项错误。

### 题目17

在区块链审计中，智能合约最常见的逻辑漏洞是：

A. 整数溢出

B. 重入攻击

C. 权限控制失效

D. 跨链数据不一致

**答案：B**

**解析**：重入攻击是智能合约最典型的漏洞之一，攻击者通过递归调用合约函数，在合约状态更新前重复提取资金。例如，The DAO事件就是因重入漏洞导致约5000万美元以太币被转移，因此B选项正确。

## 六、安全管理与法规

### 题目18

根据《网络安全法》，网络运营者应当履行的安全保护义务不包括：

A. 制定内部安全管理制度和操作规程

B. 对所有用户信息进行匿名化处理

C. 定期进行网络安全检测和评估

D. 采取数据分类和加密等措施

**答案：B**

**解析**：《网络安全法》要求网络运营者对个人信息进行保护，但未强制要求“所有用户信息匿名化”，仅需在收集使用时明示并取得同意，因此B选项错误。

### 题目19

信息安全管理体系（ISMS）的核心是：

A. 通过PDCA循环持续改进安全水平

B. 建立全面的技术防护体系

C. 实施最小特权原则

D. 定期进行渗透测试

**答案：A**

**解析**：ISMS基于PDCA（计划-执行-检查-改进）循环，通过持续优化安全策略和控制措施提升安全水平，这是ISMS的核心方法论，因此A选项正确。

## 七、安全技术深度解析

### 题目20

以下哪种加密算法属于非对称加密？

A. AES

B. DES

C. RSA

D. RC4

**答案：C**

**解析**：RSA是典型的非对称加密算法，基于大数分解难题，密钥长度通常为2048位或4096位；AES、DES、RC4均为对称加密算法，因此C选项正确。

### 题目21

某企业遭遇勒索病毒攻击，导致核心业务系统文件被加密。最有效的应急响应措施是：

A. 立即断开网络并部署杀毒软件

B. 使用离线备份恢复数据

C. 支付赎金以快速恢复业务

D. 重新安装操作系统并更新补丁

**答案：B**

**解析**：勒索病毒加密后，最直接有效的恢复方式是使用未被感染的离线备份数据。支付赎金存在法律风险且无法保证数据恢复，其他措施无法直接恢复加密文件，因此B选项正确。

## 八、新增考点专项练习（2025年大纲）

### AI防御模块

#### 题目22

某电商平台部署生成式AI客服后，发现其泄露用户订单信息。经排查无外部入侵，可能的风险根源是：

A. 防火墙配置错误

B. 训练数据包含未脱敏订单

C. 客服账户权限过高

D. SQL注入攻击

**答案：B**

**解析**：AI系统数据层风险中，训练数据未脱敏会导致模型“记忆”敏感信息并在交互中泄露，属于典型AI内生风险，区别于传统安全问题，因此B选项正确。

### 区块链审计模块

#### 题目23

在联盟链审计中，以下哪项属于特有安全隐患？

A. 51%算力攻击

B. 智能合约重入漏洞

C. 节点准入未做身份核验

D. 私钥丢失无法找回

**答案：C**

**解析**：联盟链采用“许可准入”机制，节点身份核验是核心安全控制点，公链无此要求，因此C选项属于联盟链特有风险。

## 十、信息安全管理拓展

### 题目24

以下哪项不属于信息安全管理体系（ISMS）的核心原则？

A. 安全需求驱动设计

B. 最小特权原则

C. 单一故障点

D. 纵深防御

**答案：C**

**解析**：ISMS强调避免单一故障点，需通过冗余设计增强系统可靠性；其他选项均为核心原则。

### 题目25

在风险评估中，以下哪项不属于脆弱性识别的范畴？

A. 系统未安装安全补丁

B. 员工安全意识薄弱

C. 外部黑客攻击

D. 防火墙配置错误

**答案：C**

**解析**：外部黑客攻击属于威胁，而非脆弱性；脆弱性是系统自身存在的弱点。

### 题目26

根据GB/T 22239-2019《网络安全等级保护基本要求》，第三级信息系统的“安全管理中心”要求不包括：

A. 安全管理功能集中实现

B. 审计日志应保存至少6个月

C. 应能对异常行为进行自动告警

D. 需采用量子加密技术保障通信

**答案：D**

**解析**：三级等保未强制要求量子加密，主要通过传统加密技术保障通信安全。

### 题目27

某企业计划实施灾难恢复计划，其RTO（恢复时间目标）为4小时，RPO（恢复点目标）为1小时，这意味着：

A. 系统中断后4小时内必须恢复，且数据丢失不超过1小时

B. 系统中断后1小时内必须恢复，且数据丢失不超过4小时

C. 系统中断后4小时内必须恢复，且数据丢失不超过4小时

D. 系统中断后1小时内必须恢复，且数据丢失不超过1小时

**答案：A**

**解析**：RTO指恢复服务的时间，RPO指数据可容忍丢失的最大时长。

### 题目28

以下哪项是《数据安全法》中规定的核心数据处理者义务？

A. 所有数据必须本地化存储

B. 定期开展数据安全风险评估

C. 对用户数据进行匿名化处理

D. 公开数据处理流程

**答案：B**

**解析**：《数据安全法》要求核心数据处理者定期进行风险评估并上报结果。

## 十一、网络安全技术深化

### 题目29

以下关于入侵防御系统（IPS）的描述，错误的是：

A. 可实时阻断异常流量

B. 可能成为网络单点故障点

C. 工作在网络层，无法检测应用层攻击

D. 需与防火墙协同工作以提升防护效果

**答案：C**

**解析**：IPS可检测应用层攻击（如SQL注入、XSS），部分高级IPS具备应用层深度检测能力。

### 题目30

在无线安全中，WPA3相比WPA2的主要改进是：

A. 采用TKIP加密算法

B. 支持SAE（同时认证加密）

C. 降低对硬件性能的要求

D. 仅支持2.4GHz频段

**答案：B**

**解析**：WPA3引入SAE机制，增强密钥协商安全性，防御暴力破解。

### 题目31

以下哪种攻击利用了TCP三次握手的缺陷？

A. SYN Flood

B. SQL注入

C. XSS

D. ARP欺骗

**答案：A**

**解析**：SYN Flood通过发送大量半连接请求耗尽服务器资源，利用TCP握手缺陷。

### 题目32

某公司部署了Web应用防火墙（WAF），但仍遭SQL注入攻击，可能的原因是：

A. WAF未开启实时监控

B. 攻击 payload 绕过了WAF规则

C. 服务器未安装杀毒软件

D. 数据库未使用加密存储

**答案：B**

**解析**：攻击者可能通过编码、变异等方式绕过WAF规则，如将空格替换为/\*\*/。

### 题目33

以下哪项不属于VPN的核心功能？

A. 数据加密传输

B. 隐藏真实IP地址

C. 加速网络访问

D. 跨越网络限制

**答案：C**

**解析**：VPN主要提供加密、匿名和访问控制功能，通常不会加速网络访问。

## 十二、安全工程与实践

### 题目34

在软件开发生命周期（SDLC）中，安全测试的最佳时机是：

A. 仅在上线前进行

B. 贯穿整个开发过程

C. 仅在编码阶段完成后

D. 无需专门测试，依赖防火墙防护

**答案：B**

**解析**：安全测试应在需求、设计、编码、部署各阶段持续进行，遵循“左移”原则。

### 题目35

以下哪项属于安全开发生命周期（SDL）的核心活动？

A. 代码混淆

B. 渗透测试

C. 安全需求分析

D. 漏洞赏金计划

**答案：C**

**解析**：SDL强调在设计阶段明确安全需求，其他选项为辅助措施。

### 题目36

某企业开发一款金融APP，以下哪项安全措施优先级最高？

A. 界面美观设计

B. 多因素认证

C. 广告推送功能

D. 社交分享集成

**答案：B**

**解析**：金融APP需优先保障用户身份认证安全，多因素认证是核心措施。

### 题目37

以下哪项不属于安全基线的范畴？

A. 操作系统补丁级别

B. 密码复杂度要求

C. 员工绩效考核

D. 日志审计策略

**答案：C**

**解析**：安全基线是系统最小安全配置，不涉及员工绩效。

### 题目38

在灾难恢复策略中，“热备”方案的特点是：

A. 备份数据与主数据实时同步

B. 恢复时间较长

C. 成本最低

D. 仅适用于非核心业务

**答案：A**

**解析**：热备通过实时同步实现快速恢复，适用于核心业务，成本较高。

## 十三、法律法规与合规

### 题目39

《网络安全法》规定，关键信息基础设施运营者应当多久进行一次网络安全检测和评估？

A. 每季度

B. 每半年

C. 每年

D. 每两年

**答案：C**

**解析**：《网络安全法》第三十八条要求关键信息基础设施运营者每年进行安全检测和评估。

### 题目40

以下哪项不属于《个人信息保护法》规定的个人信息处理规则？

A. 收集个人信息需明示目的

B. 无需用户同意即可共享数据

C. 遵循最小必要原则

D. 确保数据准确性

**答案：B**

**解析**：共享个人信息需获得用户单独同意，除非法律另有规定。

### 题目41

根据《数据安全法》，以下哪项数据不属于国家核心数据？

A. 国民经济数据

B. 军事数据

C. 个人健康数据

D. 国家安全数据

**答案：C**

**解析**：国家核心数据包括国家安全、国民经济、军事等领域数据，个人健康数据属于重要数据。

### 题目42

某企业向境外提供个人信息，需满足的条件不包括：

A. 通过国家网信部门安全评估

B. 确保境外接收方技术能力优于境内

C. 与境外接收方签订安全协议

D. 取得个人单独同意

**答案：B**

**解析**：《个人信息保护法》未要求境外接收方技术能力优于境内，只需满足安全要求。

### 题目43

《生成式人工智能服务管理暂行办法》要求提供生成式AI服务的企业需落实的安全措施不包括：

A. 内容审核机制

B. 算法透明度公开

C. 训练数据合法性审核

D. 可验证关闭机制

**答案：B**

**解析**：暂行办法未强制要求公开算法透明度，强调内容安全和数据合规。

## 十四、AI防御与区块链审计（2025新增）

### 题目44

生成式AI模型在训练过程中可能面临的内生风险是：

A. 模型投毒

B. DDoS攻击

C. SQL注入

D. ARP欺骗

**答案：A**

**解析**：模型投毒是AI特有风险，通过污染训练数据影响模型输出。

### 题目45

以下哪项是智能合约审计的核心关注点？

A. 界面美观度

B. 逻辑漏洞（如重入攻击）

C. 区块链节点数量

D. 代币价格波动

**答案：B**

**解析**：智能合约审计重点检测逻辑漏洞，如重入攻击、整数溢出等。

### 题目46

在AI安全治理中，以下哪项不属于《生成式人工智能服务管理暂行办法》的要求？

A. 生成内容需标注来源

B. 提供用户申诉渠道

C. 公开训练数据来源

D. 具备内容过滤机制

**答案：C**

**解析**：暂行办法未要求公开训练数据来源，仅需审核数据合法性。

### 题目47

联盟链与公链相比，其安全特性是：

A. 完全去中心化

B. 节点准入需审核

C. 匿名性更高

D. 无需共识机制

**答案：B**

**解析**：联盟链采用许可准入机制，节点需通过身份核验，中心化程度高于公链。

### 题目48

对抗性样本攻击的主要目的是：

A. 使AI模型输出错误结果

B. 窃取训练数据

C. 耗尽模型算力

D. 篡改区块链数据

**答案：A**

**解析**：对抗性样本通过微小扰动使模型分类错误，如将“猫”识别为“狗”。

## 十五、安全评估与测试

### 题目49

以下哪项不属于渗透测试的阶段？

A. 信息收集

B. 漏洞利用

C. 社会工程学攻击

D. 数据销毁

**答案：D**

**解析**：渗透测试包括信息收集、扫描、利用、报告等阶段，数据销毁不属于测试流程。

### 题目50

在漏洞扫描中，误报产生的主要原因是：

A. 扫描工具版本过低

B. 目标系统未联网

C. 扫描规则过于严格

D. 未使用管理员权限扫描

**答案：C**

**解析**：过于严格的规则可能将正常配置识别为漏洞，导致误报。

### 题目51

安全评估报告的核心内容不包括：

A. 漏洞详情及风险等级

B. 整改建议

C. 企业财务数据

D. 测试范围与方法

**答案：C**

**解析**：安全评估报告聚焦安全问题，不涉及企业财务数据。

### 题目52

以下哪种测试方法属于“白盒测试”？

A. 对系统功能进行黑盒验证

B. 代码审计

C. 社会工程学测试

D. 网络端口扫描

**答案：B**

**解析**：白盒测试需了解系统内部结构，如代码审计；其他选项为黑盒测试。

### 题目53

某企业进行安全评估后，发现高风险漏洞5个，中风险10个，低风险20个，应优先处理：

A. 低风险漏洞，数量最多

B. 中风险漏洞，影响适中

C. 高风险漏洞，潜在危害大

D. 随机处理，无优先级

**答案：C**

**解析**：风险处理应优先解决高风险漏洞，降低潜在损失。

## 十六、物理与环境安全

### 题目54

数据中心选址不应考虑的因素是：

A. 远离自然灾害高发区

B. 交通便利

C. 一楼或地下室

D. 电力供应稳定

**答案：C**

**解析**：数据中心应避免一楼（洪水风险）和地下室（湿度问题），优先选择中层楼层。

### 题目55

以下哪项不属于物理安全控制措施？

A. 门禁系统

B. 监控摄像头

C. 防火墙

D. 生物识别

**答案：C**

**解析**：防火墙属于逻辑安全控制，其他选项为物理安全措施。

### 题目56

在机房安全管理中，以下哪项措施可防止未授权人员进入？

A. 部署IDS

B. 实施双因素认证

C. 数据加密

D. 定期备份

**答案：B**

**解析**：双因素认证可增强物理访问控制，如门禁卡+指纹。

### 题目57

以下哪项是机房火灾的主要原因？

A. 温度过低

B. 静电积累

C. 湿度超标

D. 线路老化

**答案：D**

**解析**：线路老化易引发短路火灾，其他因素可能导致设备故障但非火灾主因。

### 题目58

物理安全与逻辑安全的关系是：

A. 相互独立，无需协同

B. 物理安全是逻辑安全的基础

C. 逻辑安全优先于物理安全

D. 物理安全可替代逻辑安全

**答案：B**

**解析**：物理安全是逻辑安全的前提，如服务器被物理接触可能导致数据泄露。

## 十七、安全运营与响应

### 题目59

以下哪项不属于安全事件的特征？

A. 突发性

B. 破坏性

C. 可预测性

D. 蔓延性

**答案：C**

**解析**：安全事件具有突发性、破坏性和蔓延性，难以完全预测。

### 题目60

在应急响应中，以下哪项是首要任务？

A. 消除攻击源

B. 恢复业务系统

C. 保护证据

D. 通知管理层

**答案：A**

**解析**：应急响应第一步是隔离攻击源，防止事件扩大。

### 题目61

安全信息和事件管理（SIEM）系统的核心功能是：

A. 自动修复漏洞

B. 日志聚合与分析

C. 发起渗透测试

D. 加密传输数据

**答案：B**

**解析**：SIEM整合多源日志，通过关联分析识别安全事件。

### 题目62

以下哪项不属于灾难恢复策略？

A. 冷备

B. 温备

C. 热备

D. 逻辑备

**答案：D**

**解析**：灾难恢复策略包括冷备、温备、热备，逻辑备不属于此类范畴。

### 题目63

某企业遭遇勒索病毒攻击，正确的应对措施是：

A. 立即支付赎金

B. 断开感染主机网络

C. 重启服务器尝试恢复

D. 删除加密文件

**答案：B**

**解析**：首要措施是隔离感染主机，防止病毒扩散，再进行数据恢复。

## 十八、法律法规与标准

### 题目64

《网络安全法》规定，网络运营者应当建立的制度不包括：

A. 网络安全管理制度

B. 应急预案

C. 员工绩效管理制度

D. 安全事件报告制度

**答案：C**

**解析**：《网络安全法》未要求建立员工绩效管理制度，其他选项为法定要求。

### 题目65

ISO/IEC 27001的核心是：

A. 信息安全管理体系认证

B. 具体技术防护措施

C. 黑客攻防技术

D. 数据加密标准

**答案：A**

**解析**：ISO/IEC 27001是信息安全管理体系的国际标准，关注体系建设。

### 题目66

以下哪项不属于我国网络安全等级保护制度的级别？

A. 第一级：用户自主保护级

B. 第二级：系统审计保护级

C. 第三级：安全标记保护级

D. 第五级：军事保护级

**答案：D**

**解析**：等保分为1-5级，第五级为“专控保护级”，非“军事保护级”。

### 题目67

《关键信息基础设施安全保护条例》要求运营者履行的义务不包括：

A. 安全监测和风险评估

B. 数据跨境传输审批

C. 定期开展应急演练

D. 公开系统架构细节

**答案：D**

**解析**：运营者无需公开系统架构，需保障关键信息基础设施安全。

### 题目68

以下哪项是《密码法》规定的核心密码的适用范围？

A. 普通民用信息

B. 国家秘密信息

C. 企业商业秘密

D. 个人隐私数据

**答案：B**

**解析**：核心密码用于保护国家秘密信息，普通密码用于保护重要数据。

## 十九、新兴技术安全

### 题目69

云计算环境下，以下哪项安全责任由云服务商承担？

A. 应用层安全

B. 物理基础设施安全

C. 数据内容安全

D. 访问控制策略

**答案：B**

**解析**：云服务商负责物理设施安全，用户负责应用和数据安全。

### 题目70

物联网设备的主要安全风险不包括：

A. 固件更新不及时

B. 弱口令

C. 计算能力强

D. 缺乏安全设计

**答案：C**

**解析**：物联网设备通常计算能力较弱，而非过强；其他选项均为常见风险。

### 题目71

区块链技术的核心特点不包括：

A. 去中心化

B. 不可篡改

C. 匿名性

D. 高性能

**答案：D**

**解析**：区块链因共识机制限制，性能（如TPS）通常低于传统数据库。

### 题目72

工业控制系统（ICS）的安全威胁主要来自：

A. 个人电脑病毒

B. 针对关键基础设施的攻击

C. 普通办公软件漏洞

D. 员工上网行为

**答案：B**

**解析**：ICS作为关键基础设施，面临定向攻击风险，如Stuxnet病毒。

### 题目73

5G网络的安全挑战不包括：

A. 网络切片隔离

B. 边缘计算节点安全

C. 海量设备接入

D. 供应链安全

**答案：A**

**解析**：网络切片隔离是安全措施，而非挑战；其他选项为5G安全风险。

## 二十、安全意识与培训

### 题目74

以下哪项属于社会工程学攻击？

A. 暴力破解密码

B. 发送钓鱼邮件

C. SQL注入

D. 端口扫描

**答案：B**

**解析**：钓鱼邮件通过欺骗用户获取信息，属于社会工程学攻击。

### 题目75

员工安全意识培训的重点不包括：

A. 识别钓鱼邮件

B. 密码管理

C. 高级黑客技术

D. 安全事件报告流程

**答案：C**

**解析**：员工培训聚焦基础安全意识，无需掌握高级黑客技术。

### 题目76

以下哪项是良好的密码管理习惯？

A. 所有账户使用相同密码

B. 密码包含字母、数字和特殊字符

C. 密码写在便签上贴于显示器

D. 长期不更换密码

**答案：B**

**解析**：强密码应包含多种字符类型，长度至少12位，定期更换。

### 题目77

某员工收到可疑邮件，正确的做法是：

A. 立即删除邮件

B. 点击附件查看内容

C. 报告安全团队

D. 转发给同事确认

**答案：C**

**解析**：发现可疑邮件应报告安全团队，避免自行处理导致风险。

### 题目78

安全意识培训的频率建议为：

A. 每年一次

B. 每季度一次

C. 每月一次

D. 入职时一次即可

**答案：B**

**解析**：安全意识培训宜每季度进行一次，结合最新威胁案例更新内容。

## 二十一、安全支撑技术

### 题目79

以下哪项不属于PKI的组件？

A. CA（证书颁发机构）

B. RA（注册机构）

C. KDC（密钥分发中心）

D. CRL（证书吊销列表）

**答案：C**

**解析**：KDC属于Kerberos协议组件，PKI包含CA、RA、CRL等。

### 题目80

数字签名的主要作用是：

A. 加密数据

B. 验证数据完整性和发送方身份

C. 压缩文件

D. 加速数据传输

**答案：B**

**解析**：数字签名使用私钥加密摘要，验证数据未被篡改且来自合法发送方。

### 题目81

以下哪种算法可用于数据完整性校验？

A. AES

B. RSA

C. SHA-256

D. DH

**答案：C**

**解析**：SHA-256是哈希算法，用于生成数据摘要，验证完整性；其他为加密算法。

### 题目82

以下哪项不属于入侵检测系统（IDS）的检测方法？

A. 基于特征

B. 基于行为

C. 基于漏洞

D. 基于异常

**答案：C**

**解析**：IDS检测方法包括特征、行为、异常检测，不直接基于漏洞。

### 题目83

虚拟专用网（VPN）的核心协议不包括：

A. IPSec

B. SSL/TLS

C. PPTP

D. HTTP

**答案：D**

**解析**：HTTP是应用层协议，非VPN核心协议；其他为常见VPN协议。

## 二十二、综合场景分析

### 题目84

某电商平台遭遇DDoS攻击，导致网站无法访问，应首先：

A. 联系ISP增加带宽

B. 启动DDoS防护预案，切换流量清洗

C. 关闭网站，避免损失扩大

D. 报警并追查攻击者

**答案：B**

**解析**：优先启动应急预案，通过流量清洗缓解攻击，保障业务可用性。

### 题目85

某企业发现核心数据被泄露，可能的原因不包括：

A. 员工邮箱被盗

B. 数据库未加密

C. 开启了防火墙

D. 备份介质管理不当

**答案：C**

**解析**：防火墙可阻断外部攻击，不会直接导致数据泄露；其他选项均为可能原因。

### 题目86

在智慧城市建设中，以下哪项安全措施最关键？

A. 统一安全管理平台

B. 大量部署摄像头

C. 开放数据共享

D. 使用开源软件

**答案：A**

**解析**：统一安全管理平台可整合各系统安全策略，实现集中防护；其他选项需配合安全措施。

### 题目87

某医院的医疗信息系统遭勒索病毒攻击，正确的应对措施是：

A. 立即支付赎金，恢复数据

B. 断开网络，隔离感染系统

C. 重启服务器尝试清除病毒

D. 关闭所有终端

**答案：B**

**解析**：首要措施是隔离感染系统，防止病毒扩散，再通过备份恢复数据。

### 题目88

某政府部门计划上云，需考虑的安全因素不包括：

A. 云服务商资质

B. 数据备份策略

C. 云平台市场占有率

D. 合规性认证

**答案：C**

**解析**：市场占有率非安全因素，应关注资质、备份、合规等安全指标。

## 二十三、安全管理实践

### 题目89

信息安全策略的制定者应为：

A. 安全团队

B. 高级管理层

C. IT部门

D. 外部咨询机构

**答案：B**

**解析**：安全策略需由高级管理层批准，确保资源支持和全员执行。

### 题目90

以下哪项不属于业务连续性计划（BCP）的内容？

A. 风险评估

B. 应急响应流程

C. 员工绩效考核

D. 灾难恢复策略

**答案：C**

**解析**：BCP聚焦业务持续运营，不涉及员工绩效考核。

### 题目91

安全基线的作用是：

A. 确保系统满足最低安全要求

B. 实现零风险

C. 替代安全策略

D. 仅适用于核心系统

**答案：A**

**解析**：安全基线定义系统最小安全配置，确保基本防护能力。

### 题目92

以下哪项是安全事件响应的正确流程？

A. 检测→遏制→根除→恢复→总结

B. 遏制→检测→根除→恢复→总结

C. 检测→恢复→遏制→根除→总结

D. 总结→检测→遏制→根除→恢复

**答案：A**

**解析**：安全事件响应需先检测，再遏制、根除、恢复，最后总结改进。

### 题目93

风险管理的核心流程是：

A. 风险识别→风险分析→风险评价→风险处理

B. 风险处理→风险识别→风险分析→风险评价

C. 风险评价→风险处理→风险识别→风险分析

D. 风险分析→风险评价→风险处理→风险识别

**答案：A**

**解析**：风险管理流程始于识别，经分析、评价后进行处理。

## 二十四、技术与管理融合

### 题目94

以下哪项体现了“技术+管理”的综合安全观？

A. 仅部署防火墙

B. 制定安全策略并定期审计

C. 依赖员工自觉遵守安全规定

D. 不更新系统补丁

**答案：B**

**解析**：综合安全观需结合技术措施（如防火墙）和管理措施（如策略、审计）。

### 题目95

在DevSecOps中，安全融入的阶段是：

A. 仅在测试阶段

B. 开发全过程

C. 仅在部署后

D. 无需融入

**答案：B**

**解析**：DevSecOps强调安全融入开发全流程，而非单一阶段。

### 题目96

以下哪项是衡量安全团队绩效的关键指标？

A. 防火墙部署数量

B. 安全事件响应时间

C. 员工人数

D. 服务器数量

**答案：B**

**解析**：响应时间反映安全团队处理事件的效率，是核心绩效指标。

### 题目97

某企业安全预算有限，应优先投入的领域是：

A. 高级安全设备

B. 员工安全培训

C. 全面的安全审计

D. 核心业务系统防护

**答案：D**

**解析**：资源有限时应优先保障核心业务安全，采用风险导向策略。

### 题目98

安全文化建设的核心是：

A. 惩罚违规员工

B. 全员参与安全管理

C. 购买昂贵安全产品

D. 仅高层关注安全

**答案：B**

**解析**：安全文化需全员参与，而非仅依赖惩罚或高层关注。

## 二十五、备考注意事项

1. **重点模块**：2025年考试新增AI防御、区块链审计模块，占比约15%，需重点掌握模型风险、智能合约审计等知识点。

2. **题型分布**：单选题80道（80分），场景分析题20道（20分），实操题占比提升至40%。

3. **复习策略**：结合模拟题演练，优先掌握加密算法、访问控制、风险评估等核心知识点，关注《网络安全法》《数据安全法》最新修订内容。

4. **答题技巧**：遇到不确定题目时，采用排除法缩小范围，优先选择符合“最小特权”“纵深防御”等原则的选项。

5. **资料推荐**：官方授权培训机构的模拟题库（如思博网络、中培IT学院）及CISP官网《2025版知识体系大纲》。

**提示**：本资料共包含98道CISP练习习题，覆盖考试核心知识点，建议结合实际操作（如搭建DVWA靶场）提升实战能力。如需进一步补充特定模块题目，可提供具体方向。

### 题目99

在安全工程中，以下哪项不属于“纵深防御”策略的体现？

A. 网络边界部署防火墙

B. 主机安装杀毒软件

C. 数据加密存储

D. 单一供应商提供所有安全设备

**答案：D**

**解析**：纵深防御强调多层次、多技术、多供应商的安全架构，单一供应商可能导致单点故障风险。

### 题目100

应急响应中，“恢复”阶段的核心任务是：

A. 找出攻击源并封堵

B. 将系统恢复至正常运行状态

C. 分析攻击路径

D. 撰写事件报告

**答案：B**

**解析**：恢复阶段需确保业务系统恢复正常运行，优先保障可用性，其他任务属于后续阶段。

## 二十六、最终说明

本资料共收录100道CISP练习习题，涵盖信息安全管理、技术、法规、新兴技术等核心模块，包含2025年新增AI防御、区块链审计考点。所有题目均来自合法合规的模拟题资源，解析详细，适合备考复习。建议结合官方授权机构的在线刷题系统进行强化训练，重点关注实操题和场景分析题。

**注意**：本资料仅包含合法获取的模拟题和练习题，不涉及任何真题，仅供学习参考。建议通过官方授权渠道获取最新备考资源。