TRACCIA n. 1 (ESTRATTA):

Quesito n. 1: Con riferimento alla definizione, progettazione e implementazione di soluzioni di sicurezza per infrastrutture complesse e per la protezione di sistemi informatici e tecnologici, fornire una descrizione dei requisiti chiave di sicurezza quali confidenzialità, integrità e disponibilità ad esse associate, spiegandone ruoli e obiettivi e fornendo alcuni esempi, possibilmente in ambito di progetti spaziali.

Quesito n. 2: Nel contesto della sicurezza delle reti informatiche, la protezione delle comunicazioni riveste un ruolo fondamentale. Essa comprende misure contro attacchi passivi (come intercettazione e analisi del traffico) e attacchi attivi (come mascheramento e alterazione dei dati). A tal fine, vengono adottati protocolli di sicurezza che definiscono il formato, le procedure e le modalità di trasmissione e ricezione dei dati tra i nodi della rete. Si richiede di elencare e descrivere i principali protocolli di sicurezza delle comunicazioni conosciuti, evidenziandone le caratteristiche distintive e le principali differenze (es. livello OSI, requisiti di sicurezza soddisfatti, robustezza, ambito d'uso, etc.).

Quesito n. 3: Con riferimento al DPCM n. 5/2015 e successiva variante di cui al DPCM n.3/2017 si diano le definizioni di "sicurezza fisica", "INFOSEC", TEMPEST" e "sicurezza cibernetica". Per ognuna di essa si provi a riportarne un esempio e/o applicazione nell'ambito di una struttura organizzativa aziendale.

TRACCIA n. 2:

Quesito n. 1: Con riferimento alla definizione, progettazione e implementazione di soluzioni di sicurezza per infrastrutture complesse e per la protezione di sistemi informatici e tecnologici, fornire una descrizione dei requisiti chiave di sicurezza quali confidenzialità, integrità, disponibilità e non ripudio ad esse associate, spiegandone ruoli e obiettivi e fornendo alcuni esempi, possibilmente in ambito di progetti spaziali.

Quesito n. 2: Nell'ambito di una rete aziendale o di Internet sono presenti diverse problematiche di sicurezza che riguardano i vari endpoint della rete, come server, workstation e dispositivi mobili. Descrivere quali rischi concreti possono colpire un endpoint non protetto (ad esempio malware, accessi non autorizzati o perdita di dati) e illustrare quali misure di sicurezza possono ridurre queste minacce.

Quesito n. 3: Con riferimento al DPCM n. 5/2015 e successiva variante di cui al DPCM n.3/2017 si diano le definizioni di "violazioni di sicurezza", "INFOSEC", "COMSEC" e "sicurezza cibernetica". Per ognuna di essa si provi a riportarne un esempio e/o applicazione nell'ambito di una struttura organizzativa aziendale.

TRACCIA n. 3:

Quesito n. 1: Con riferimento alla definizione, progettazione e implementazione di soluzioni di sicurezza per infrastrutture complesse e per la protezione di sistemi informatici e tecnologici, fornire una descrizione dei requisiti chiave di sicurezza quali confidenzialità, integrità, disponibilità e autenticità ad esse associate, spiegandone ruoli e obiettivi e fornendo alcuni esempi, possibilmente in ambito di progetti spaziali.

Quesito n. 2: Fornire la descrizione di un modello di sicurezza informatica ad alto livello, illustrando le relazioni tra i principali elementi e, sulla base di tale modello, si ipotizzi la gestione e il coordinamento di attività e procedure per affrontare un incidente di sicurezza cibernetica, alla luce delle vigenti normative, degli standard internazionali e delle best practice di settore.

Quesito n. 3: Con riferimento al DPCM n. 5/2015 e successiva variante di cui al DPCM n.3/2017 si diano le definizioni di "sicurezza fisica", "Comunication Information System (CIS)", "TEMPEST" e "sicurezza cibernetica". Per ognuna di essa si provi a riportarne un esempio e/o applicazione nell'ambito di una struttura organizzativa aziendale.