Domande Esame

Appello 20 giugno 2022 - T1

(1 - M1.3.2.1) Un Protocollo di Comunicazione:

- ? È un insieme di regole definite mediante specifiche sequenze di istruzioni, di varia tipologia e finalità in base alle entità interessate e al mezzo di comunicazione
- ? Permette la comunicazione tra due o più entità connesse su una architettura di rete o di comunicazione
- ? È un insieme di regole definite mediante specifiche sequenze di istruzioni che possono essere implementate diversamente sulle varie entità interessate alla comunicazione
- ? Può essere uno standard con cui sono definiti la sintassi, la semantica e la sincronizzazione della comunicazione
- ? Può essere implementato da hardware o software o in una combinazione di entrambi

(2- M1.3.2.4) L'interfaccia USB

- ? Può raggiungere una velocità di trasmissione di 20Gbit/sec
- ? È utilizzata principalmente come interfaccia punto-punto
- ? Può gestire al massimo 10 Hub concentratori
- ? Ha tra le caratteristiche fondamentali la capacità di alimentare i dispositivi collegati
- ? Può trasmette sino ad una distanza non superiore ai 5 metri
- ? È uno standard che ha raggiunto il limite massimo di potenzialità

(3- M1.3.2.7) La modalità di trasmissione su canali in fibra ottica (WDM) è

- ? Una trasmissione bidirezionale simultanea su cavo singolo
- ? Una trasmissione bidirezionale non simultanea su cavo singolo
- ? Una modalità di trasmissione con fasci a lunghezza d'onda differente
- ? Una modalità di trasmissione con fasci di colori diversi ma con la stessa frequenza
- ? Una tecnica di trasmissione con multiplexing a divisione di ampiezza
- ? Una tecnica di trasmissione con multiplexing a divisione di lunghezza d'onda

(4- M1.3.2.10) Il Dominio di Collisione o Collision Domain nella trasmissione Ethernet:

- È un insieme di nodi, ridotto rispetto al dominio dell'intera rete locale, che concorrono per accedere allo stesso mezzo trasmissivo e quindi trasmettere
- È una tecnica per ridurre la probabilità di collisioni al crescere del numero di stazioni e/o del traffico all'interno di una LAN
- Una tecnica per evitare che in una rete LAN il mezzo trasmissivo sia condiviso e conteso per la trasmissione tra tutte le stazioni
- Una tecnica per eliminare completamente le collisioni in una comunicazione all'interno di un'unica LAN
- Una tecnica statistica per gestire le collisioni all'interno di una LAN
- La suddivisione della rete in più sottoreti in modo che la contesa del mezzo avvenga soltanto tra le stazioni appartenenti ad una singola sottorete

(5- M1.3.3.1) La convergenza funzionale:

- È la tendenza ad aumentare le funzionalità dei dispositivi di rete «inglobando» funzionalità di altre tipologie di dispositivi
- È un fenomeno causato dalla forte concorrenza sul mercato dei dispositivi di rete e dall'aumento delle prestazioni delle piattaforme di elaborazione
- È un fenomeno che non ha impatto sulla standardizzazione degli specifici brand commerciali
- È un fenomeno che ha portato all'obsolescenza di alcuni dispositivi
- È un fenomeno che ha portato alcuni switch a gestire parzialmente o totalmente funzioni di routing (livello 3 ISO/OSI)
- Ha causato l'obsolescenza dei router

(6- M1.3.3.4) Il Router:

- Gestisce il traffico trasmesso su mezzi trasmissivi differenti (esempio fibra, doppino telefonico o wi-fi)
- Attraverso l'instradamento (routing) connette dispositivi su reti differenti
- Può funzionare solo a livello 2 dello stack ISO-OSI
- Funziona normalmente a livello 3 dello stack ISO-OSI
- Gestisce il traffico attraverso l'uso degli indirizzi IP
- Gestisce il traffico attraverso l'uso degli indirizzi MAC

(7- M2.1.1.2) Quali tra questi elementi possono essere solo interni all'azienda:

- Acquisti
- Fornitore di metallo

- Qualità
- Risorse Umane
- Produzione di un semilavorato a basso valore aggiunto
- Amministrazione/Contabilità

(8- M2.1.2.2) Il Soggetto Giuridico:

- È la persona nel cui nome l'attività aziendale è esercitata
- È la persona che assume solo gli obblighi derivanti dalle operazioni aziendali
- È la persona alla quale sono riferiti i diritti e gli obblighi che nascono dalla costituzione dell'azienda e dal suo esercizio
- Può essere una Persona Giuridica ovvero un ente, un'azienda o una società
- Può essere solo la Persona Fisica nel cui nome l'attività aziendale è esercitata
- Può essere indifferentemente la Persona Fisica o Giuridica, entrambe hanno capacità giuridica

(9- M2.1.3.1) Le aziende nel settore terziario

- Possono realizzare attività di intermediazione, o di produzione indiretta di beni, attraverso il commercio degli stessi
- Possono realizzare attività di produzione diretta di beni
- Possono essere quelle attività complementari e di ausilio ai settori primario e secondario
- Possono realizzare produzione diretta o indiretta di servizi (ad esempio le aziende bancarie, assicurative, di trasporto, ecc.)
- Possono essere le aziende che gestiscono i trasporti e le comunicazioni
- Possono basare il proprio core business sul know-how e sui servizi intellettuali (R&D, formazione, consulenza, ecc.)

(10- M2.2.1.1) Quali dei seguenti asset possono essere affetti da problemi di Sicurezza Informatica?

(V= lo è, F= non lo è)

- Il sistema informativo gestionale
- L'Web aziendale
- Sistemi elettromeccanici meccanici non dotati, in alcun modo, di sistemi elettronici a processore
- Il CAD o il CAM (Computer Aided Design/Manufacturing)
- Apparati di produzione con sistemi operativi standard non connessi alla rete aziendale
- Il CRM (Customer Relationship Management)

(11- M2.3.1.2) Il Sistema di Gestione aziendale

- Sono modelli organizzativi aziendali adottati su base volontaria e realizzati mediante l'applicazione organica e sistematica di regole e procedure
- Sono regole e procedure che una azienda fa proprie solamente a livello di top management e di consiglio di amministrazione allo scopo di raggiungere specifici obiettivi
- Può avere come obiettivo il tenere sotto controllo l'attività dell'azienda affinché sia in grado di soddisfare le esigenze del Cliente
- Può avere come obiettivo il miglioramento progressivo delle prestazioni aziendali
- Non riguarda specificamente il controllo dei processi aziendali
- Può dimostrare a terzi, soprattutto a Organismi di controllo e potenziali clienti, la propria capacità di mantenere i propri impegni (conformità normativa)

(12- M2.3.2.2) I Processi Aziendali

- Possono essere modellizzati ed in questo modo è possibile verificare eventuali anomalie del processo stesso ed apportarne miglioramenti
- Non sempre possono essere modellizzati vista la complessità delle attività e la concatenazione di esse
- Attraverso la modellizzazione possono essere meglio compresi dal personale durante il periodo di formazione
- Possono essere modellizzati ed in questo modo è possibile salvaguardare il know how aziendale
- Una volta strutturati possono rimanere stabili decine di anni senza modifiche
- Sono utili soprattutto al top management per necessità operative

(13- M3.1.1.3) L'Evento di Sicurezza Informatica

- Può essere considerato come qualsiasi situazione che si verifichi nell'ambito di un determinato asset informatico, comunque rilevata, la cui rilevanza è considerata significativa ai fini della salvaguardia dell'infrastruttura informatica
- Può essere considerata qualsiasi situazione che sottintenda una violazione delle politiche di sicurezza IT fonte di danno per gli asset IT ovvero per il patrimonio informativo dell'organizzazione e per il quale si renda necessaria l'applicazione di misure di analisi e di contrasto e/o contenimento
- Può essere considerato come qualsiasi situazione che si verifichi nell'ambito di un determinato asset informatico, comunque rilevata, la cui rilevanza è considerata significativa ai fini delle attività di gestione, controllo della sicurezza e contenimento dei rischi ad essa correlati
- Può essere a basso impatto (non significativo): qualsiasi evento gestito in maniera silente dal sistema di sicurezza e che non richiede uno specifico trattamento
- Può essere a impatto significativo: qualsiasi evento rilevato nell'ambito dei sistemi e delle infrastrutture IT, che non necessita di essere ulteriormente analizzato

- Può essere a impatto critico: qualsiasi evento significativo che, a seguito delle analisi effettuale, potrebbe sottintendere, direttamente o indirettamente, una violazione delle politiche di sicurezza dell'azienda

(14- M3.1.3.1) La Standardizzazione:

- Si può definire come un'attività che dà origine a soluzioni codificate e ripetibili a problemi in varie discipline
- Di solito non è orientata ad un ritorno economico e di immagine
- L'attività, in generale, costituisce il processo di definizione (determinazione, formulazione e rilascio) e di implementazione degli standard
- Può essere il risultato di un'attività di razionalizzazione e può riguardare tutte le attività aziendali, a partire da quelle più critiche
- Può essere applicata, con notevoli vantaggi, nell'area della sostenibilità ambientale
- Di solito, per problematiche di complessità e costi, tendenzialmente non si applica nell'ambito della qualità

(15- M3.2.1.1) Lo standard ISO/IEC 27000-series

- È una serie di norme internazionali che costituiscono uno standard relativo alla sicurezza informatica
- È uno standard monolitico costituito da un solo documento che unisce insieme una serie di norme internazionali
- È denominato "Information Security Management Systems (ISMS) Family of Standards" e si prefigge di proteggere le informazioni che vengono mantenute ed elaborate da un'organizzazione
- Permette alle organizzazioni di sviluppare ed implementare un proprio sistema per la gestione della sicurezza informatica per le informazioni finanziarie, la proprietà intellettuale ed i dati dei dipendenti, di clienti o di terzi
- Ha generato altri standard, tra cui il British Standard BS 7799-1 e -2
- Si focalizza sulla protezione dei dati unicamente attraverso il consolidamento tecnologico

(16- M3.2.1.4) I Controlli ISO/IEC 27001 (Allegato A)

- Sono le appropriate contromisure selezionate dalle organizzazioni per affrontare i rischi per la cyber security identificati
- Come indicato nel documento ISO/IEC 27002 associato all'Annex A di ISO 27001 sono strutturati secondo uno schema a 3 livelli
- Come indicato nel documento ISO/IEC 27002 associato all'Annex A di ISO 27001 sono strutturati secondo uno schema a 2 livelli
- Sono 114 secondo l'edizione ISO/IEC 27001/2 2013
- Sono 116 secondo l'edizione ISO/IEC 27001/2 2016

- Sono 93 secondo l'edizione ISO/IEC 27002 2022

(17- M3.2.1.7) Quali delle seguenti sono Aree di Controllo secondo ISO 27001 2013?

- Sicurezza logica e ambientale
- Sicurezza delle attività operative
- Sicurezza delle reti e dei sistemi di comunicazione
- Acquisizione, sviluppo e manutenzione dei sistemi
- Gestione della catena di fornitura
- Gestione degli incidenti relativi alla sicurezza delle informazioni

(18- M3.2.3.1) Il NIST Cybersecurity Framework

- È un insieme di linee guida per mitigare i rischi di sicurezza informatica organizzativa
- È stato pubblicato dal NIST avendo come obiettivo la realizzazione di uno standard equivalente alla serie ISO/IEC 27000
- È composto da quattro parti: Framework Core, Framework Implementation Tiers, Framework Profiles e Framework Deployment
- Realizza un quadro che "fornisce una tassonomia di alto livello dei risultati relativi alla sicurezza informatica e una metodologia per valutare e gestire tali risultati"
- Realizza un quadro che "fornisce una tassonomia dettagliata dei risultati della sicurezza informatica e una valutazione di tali risultati"
- Realizza un quadro che permette orientamenti sulla protezione della privacy e delle libertà civili in un contesto di sicurezza informatica

(19- M3.2.3.4) Nel NIST CSF i livelli di implementazione del framework ("Tier")

- Forniscono un contesto su come un'organizzazione considera il rischio di sicurezza informatica e i processi in atto per gestirlo
- Descrivono il grado in cui le pratiche di gestione del rischio di sicurezza informatica di un'organizzazione esibiscono le caratteristiche definite nel Framework (ad esempio, consapevole del rischio e delle minacce, ripetibile e adattivo)
- Caratterizzano le pratiche di un'organizzazione in un intervallo, da Parziale (Tier 1) ad Adattativo (Tier 5)
- Riflettono una progressione da risposte informali e reattive (Tier 1) ad approcci agili e informati sui rischi (Tier 5)
- Durante il processo di selezione del livello, un'organizzazione dovrebbe considerare le sue attuali pratiche di gestione del rischio, l'ambiente delle minacce, i requisiti legali e normativi, gli obiettivi aziendali/della missione e i vincoli organizzativi

- Sono valutati considerando tre parametri che permettono di verificare il livello di sviluppo del Processo di Gestione del Rischio (1), l'Integrazione del Programma di Gestione del Rischio (2) all'interno della realtà aziendale e la capacità dell'organizzazione di partecipare ad un ecosistema di gestione del rischio più ampio della singola realtà aziendale (3)

(20- M3.2.3.7) Nel NIST CSF il Supply Chain Risk Management (SCRM)

- Affronta sia l'effetto di sicurezza informatica che un'organizzazione ha sulle parti esterne sia l'effetto di sicurezza informatica che le parti esterne hanno su un'organizzazione
- Può includere le attività di determinazione dei requisiti di sicurezza informatica per i fornitori
- Può includere le attività di attuazione dei requisiti di sicurezza informatica attraverso accordi formali
- È l'insieme delle attività necessarie per gestire il rischio di sicurezza informatica associato a soggetti esterni
- Può includere le attività di verifica che i requisiti di sicurezza informatica siano soddisfatti attraverso una varietà di metodologie di valutazione per i soggetti interni
- Può includere le attività di comunicazione ai fornitori di come saranno verificati e convalidati i requisiti di qualità del prodotto

(21- M3.2.6.1) La serie ISA/IEC 62443

- Fornisce un quadro flessibile per affrontare e mitigare le vulnerabilità di sicurezza attuali e future nei sistemi di controllo e automazione industriale (IACS)
- Sono standard applicabili a tutti i settori industriali e alle infrastrutture critiche
- Ha un posizionamento che scende sino a livello dell'impianto
- Ha un posizionamento che parte dal coinvolgimento dell'amministratore delegato e del consiglio di amministrazione
- È costituita da quattro famiglie di standard ancora in aggiornamento
- Non riguarda direttamente gli SCADA

(22- M3.2.6.4) Le zone secondo ISA/IEC 62443

- Dividono una architettura fisica (dispositivi di rete e connessioni) in zone omogenee raggruppando i dispositivi HW con requisiti di sicurezza comuni
- Dividono un sistema in zone omogenee raggruppando le risorse (logiche o fisiche) con requisiti di sicurezza comuni
- Hanno requisiti di sicurezza definiti da Security Level (SL), il livello richiesto per una zona è determinato dall'analisi del rischio
- Hanno confini che separano gli elementi all'interno della zona da quelli esterni
- Possono includere impianti presenti in siti fisici differenti

? Possono essere suddivise in sottozone che definiscono diversi livelli di sicurezza e quindi consentono una difesa in profondità

(23- M3.2.6.7) I Livelli di Sicurezza secondo ISA/IEC 62443-1-1

? Sono tre: 1= Basso, 2=Medio e 3=Alto

? Rappresentano un metodo qualitativo per identificare la sicurezza in ciascuna zona

? Sono tre: Target, Achieved e Capability

? Hanno tre tipologie di Livelli per la gestione continua

? Valgono per le zone ma possono essere applicati anche a componenti e sistemi anche se con un numero di livelli maggiore

? Valgono solamente per le zone e non per componenti e sistemi

(24- M3.3.1.1) Il Diritto alla Privacy

? Nasce negli Stati Uniti nel 1910 dall'istituto «diritto a essere lasciato solo» (right to be let alone) e viene elaborato in Italia dagli anni '60-'70

? Attualmente viene inteso solo nel senso di protezione dei dati personali

? Originariamente significava libertà "nel fare quello che si vuole con i propri affari privati che non coinvolgono gli altri" principio che deve confrontarsi con gli altri che impediscono all'individuo di agire da solo

? Originariamente significava libertà "nel fare quello che si vuole con i propri affari privati" senza confrontarsi con gli altri

? Attualmente viene inteso non solo nel senso di protezione dei dati personali ma anche come diritto a esprimere liberamente le proprie aspirazioni

? Nasce negli Stati Uniti nel 1890 dall'istituto «diritto a essere lasciato solo» (right to be let alone) e viene elaborato in Italia dagli anni '60-'70

(25- M3.3.3.1) La Brand Reputation

? Si riferisce al modo in cui il brand (Marchio) viene valutato da parte del pubblico

? Deve essere differenziata dalla Brand Image che risulta sviluppata e costruita dall'azienda in maniera strategica e può non corrispondere alla reale percezione del pubblico

? Si sovrappone al concetto di Brand Image che corrispondere alla reale percezione del pubblico

? Impatta direttamente l'immagine dell'azienda proprietaria del marchio

? Può non impattare direttamente l'immagine dell'azienda proprietaria del marchio

? Presuppone e dipende da "azioni concrete" che si prestano ad essere rendicontate

(26- M3.3.5.1) La Direttiva NIS (Network and Information Security)

? È il primo atto legislativo sulla sicurezza informatica approvato dall'Unione Europea

- È entrata in vigore il 6 luglio 2017
- Stabilisce l'obiettivo dell'adozione di una serie di misure di sicurezza comuni che verranno successivamente definite a discrezione dei singoli paesi
- Impone la notifica obbligatoria degli incidenti all'Autorità nazionale istituita allo scopo
- Impone la nascita di CSIRT (Computer Security Incident Response Team) nazionali, sulla base del CERT-UE
- Impone di realizzare un network nei singoli paesi che si occupi della sicurezza delle reti critiche

(27- M3.3.6.1) Il Regolamento (UE) 2016/679 GDP

- È un regolamento dell'Unione europea in materia di trattamento dei dati personali e di privacy
- È stato adottato il 27 aprile 2016, pubblicato sulla Gazzetta Ufficiale dell'Unione europea il 4 maggio ed entrato in vigore il 24 maggio 2016, operativo a partire dal 25 maggio 2018
- Ha come obiettivo primario il rafforzamento della protezione dei dati personali di cittadini dell'Unione europea (UE) e dei residenti nell'UE, solo all'interno dei confini dell'UE
- Si applica al trattamento dei dati personali delle persone fisiche e al trattamento non automatizzato dei dati conservati in un «archivio»
- Il regolamento non si applica ad imprese ed enti, organizzazioni con sede legale fuori dall'UE che trattano dati di residenti dell'Unione Europea
- Il regolamento si occupa anche dei dati personali per attività di sicurezza nazionale o di ordine pubblico

(28- M3.3.6.4) Le Figure di Riferimento per il trattamento dei dati, ai sensi del "Codice della Privacy", sono le seguenti:

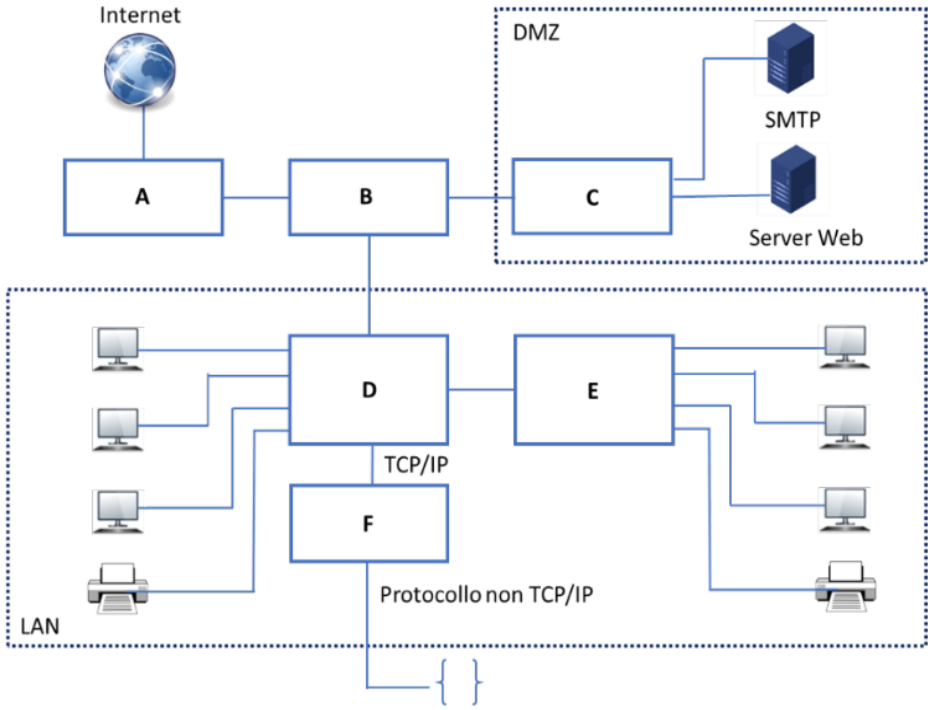
- Quattro livelli di certificazione con diverse "affidabilità"
- Tre livelli di certificazione con diverse "affidabilità"
- Un livello di affidabilità "di base", per il quale può bastare un riesame della documentazione tecnica, attività di valutazione sostitutive di effetto equivalente. Il livello base è l'unico per il quale il produttore/fornitore può ricorrere all'autocertificazione, ove prevista
- Un livello di affidabilità "sostanziale", per il quale la valutazione di sicurezza è effettuata a un livello inteso a ridurre al minimo i rischi di incidenti ed attacchi informatici commessi da soggetti che dispongono di abilità e risorse limitate
- Un livello di affidabilità "elevato, per il quale la valutazione di sicurezza è effettuata a un livello inteso a ridurre al minimo il rischio di attacchi informatici avanzati commessi da attori che dispongono di abilità e risorse significative
- Un livello di affidabilità "critico", per il quale la valutazione di sicurezza è effettuata a un livello inteso ad annullare il rischio di attacchi informatici avanzati commessi da attori che dispongono di abilità e risorse significative

(30- M3.4.3.3) Il Risk Apetite:

- Può essere tradotto come Propensione al Rischio
- Delimita inferiormente l'aerea dei rischi che devono essere assolutamente evitati o massimamente ridotti, mediante tutti gli strumenti disponibili (Area Rossa)
- Delimita superiormente l'aerea dei rischi che devono essere assolutamente evitati o massimamente ridotti, mediante tutti gli strumenti disponibili (Area Rossa)
- Delimita superiormente l'aerea dei rischi che devono essere monitorati e gestiti costantemente dall'azienda (Area Gialla)
- Indica il livello e il tipo di rischio che un'organizzazione è in grado di assumere coerentemente con gli obiettivi strategici perseguiti
- Delimita l'area di rischio entro cui l'azienda desidera muoversi

Esercizio 1

Indicare la tipologia dei dispositivi rappresentati come rettangoli nello schema seguente (Es.: Switches, Firewall, ecc.):



A. ROUTER
B. FIREWALL
C. SWITCH
D. SWITCH
E. SWITCH
F. GATEWAY

Esercizio 2

L'amministratore di una rete aziendale con indirizzo 256.18.0.0/17 desidera: (errore nell'indirizzo: 246.18.0.0/17)

- impedire l'accesso da Internet alla rete aziendale
- consentire l'accesso dalla rete 150.12.0.0/17 (rete locale della filiale) alla sottorete interna 256.18.21.0/24

- Impedire alla sottorete 150.12.10.0/24 di poter accedere alla sottorete interna 256.18.21.0/16
- Impedire alla sottorete 150.12.20.0/26 di poter accedere alla sottorete interna 256.18.21.0/16

Configurare nella seguente tabella le regole del firewall per gestire i requisiti:

Indice	IP Sorgente (o sottorete)	IP Destinatario (o sottorete)	Azione (Blocca/Consenti)
1(*)	150.12.20.0/26	256.18.21.0/16	Blocca
2(*)	150.12.10.0/24	256.18.21.0/16	Blocca
3	150.12.0.0/17	256.18.21.0/24	Consenti
4	0.0.0.0/0	0.0.0.0/0	Blocca

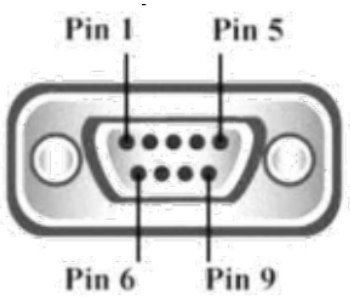
(*) Essendo sottoreti differenti le regole 1 e 2 possono essere anche invertite

Appello 20 giugno 2022 - T2

(1- M1.3.2.2) Lo Standard RS485

- ? Può raggiungere una velocità di trasmissione di 1Mb/sec
- ? Può trasmettere sino ad una distanza massima di 1.200m con specifiche velocità di trasmissione
- ? Può trasmettere sino ad una distanza massima di 5.000m con specifiche velocità di trasmissione
- ? Può supportare sino a 256 dispositivi collegati con ricevitori ad alta impedenza
- ? Può supportare sino a 1.000 dispositivi collegati con ricevitori ad alta impedenza
- ? Ha sempre un cavo con tre fili

(2- M1.3.2.5) Il connettore a 9 pin rappresentato in figura



- ? È un connettore di rete
- ? E' un connettore seriale
- ? Può essere utilizzato per RS422 e RS485
- ? Ha una piedinatura a 10 pin
- ? E' disponibile nei formati maschio/femmina

- Con piedinatura RS422/485 il connettore ha il GND (ground) sul pin 5

(3- M1.3.2.8) Un cavo in fibra ottica monomodale

- Prevede una sola modalità di propagazione: un'unica lunghezza d'onda della luce nel nucleo della fibra
- Prevede una solo modalità di propagazione: una lunghezza d'onda modulata nel tempo
- Garantisce l'assenza di interferenza o sovrapposizione tra diverse lunghezze d'onda sulle lunghe distanze
- Ha un nucleo di vetro molto più grande del cavo multimodale per garantire minore interferenza
- Ha un nucleo di vetro da 8-10 micronm (nella tipologia OS1 e OS2)
- Può essere usato, indipendentemente dalla tipologia, sia al chiuso che all'aperto

(4- M1.3.2.11) La Socket TCP è:

- Un'astrazione software standardizzata progettata per essere utilizzabile nei programmi applicativi che permette la trasmissione e la ricezione di dati attraverso una rete
- La principale responsabile nello stabilire la connessione tra due host e mantenere la sessione per poi rigenerare la connessione all'invio di ulteriori pacchetti
- Indirettamente responsabile dello hand shake a tre livelli del TCP/IP
- Direttamente responsabile dello hand shake a tre livelli del TCP/IP
- Configurata diversamente sul client e sul server
- Configurata allo stesso modo sia sul client che sul server

(5- M1.3.3.2) Lo switch di rete

- È un dispositivo elettronico che collega insieme nodi di rete
- Se di tipo "Store and Forward" può avere una latenza di trasmissione maggiore
- È un dispositivo intelligente, ovvero dotato di CPU
- Gestisce solamente il livello 2 dello stack ISO/OSI
- Non permette la segmentazione attraverso VLAN
- Se di tipo "cut-through" ha latenza minore rispetto alle altre tipologie

(6- M1.3.3.5) Il Firewall:

- È un dispositivo, esclusivamente hardware, per la sicurezza della rete
- Monitora il traffico in entrata e in uscita utilizzando una serie predefinita di regole di sicurezza per consentire o bloccare gli

eventi

- Che utilizza il criterio di applicazione “Default-Deny” permette solo ciò che viene autorizzato esplicitamente, mentre il resto viene vietato
- Che utilizza il criterio di applicazione “Default-Deny” blocca solo ciò che viene vietato esplicitamente, mentre il resto viene permesso
- Utilizza normalmente per la configurazione delle regole: indirizzo IP sorgente, IP di destinazione e la porta attraverso la quale viene erogato il servizio
- È un dispositivo che funziona solo a livello 2

(7- M2.1.1.3) Quali dei seguenti elementi possono essere classificati beni immateriali:

- Servizi erogati
- Valore del sito produttivo
- Know-how
- Concessioni esclusive
- Valore delle materie prime
- Proprietà intellettuali o brevetti

(8- M2.1.2.3) Il Soggetto Economico

- È chi, in un’azienda, possiede il potere decisionale o di conduzione dell’azienda
- È chi ha privilegi economici nell’azienda
- È chi ha il potere di indirizzo dell'attività aziendale
- È presente solo nelle aziende di produzione
- È chi riceve gli utili dell’attività aziendale anche se non partecipa alle decisioni o alla conduzione dell’azienda
- Può essere associato sia ad una persona fisica che a un gruppo di persone all’interno dell’azienda

(9- M2.1.3.2) La Utility

- È un’azienda di servizio pubblico
- Può erogare qualunque tipo di servizio basta che sia rivolto alla collettività
- Eroga, in regime di monopolio o quasi-monopolio, beni e servizi essenziali per la collettività
- Non è soggetta a nessuna regolamentazione da parte dei poteri pubblici perché opera in regime di libero mercato
- È soggetta ad una particolare regolamentazione da parte dei poteri pubblici, sia nella gestione sia nella fissazione delle tariffe
- Può erogare servizi come la fornitura di energia, la fornitura di acqua potabile e lo smaltimento dei rifiuti

(10- M2.2.2.1) Il vettore di attacco

- È il veicolo che trasporta uno o più strumenti utilizzati per realizzare un attacco che sfrutta una o più debolezze o vulnerabilità
- È la tecnica che permette un attacco con l'attaccante fisicamente dall'interno del perimetro di rete aziendale
- Per esteso può essere anche la tecnica utilizzata per l'accesso non autorizzato da parte di un malintenzionato ad un dispositivo o una rete per scopi nefasti
- Può sfruttare una rete, un computer o un dispositivo
- Sfrutta unicamente accessi esterni attraverso i portali web
- È il veicolo (o la tecnica) che può sfruttare debolezze umane come mancanza di conoscenza o attenzione

(11- M2.3.1.3) Il Sistema Informativo aziendale

- È quell'insieme di elementi che raccolgono, elaborano, memorizzano e distribuiscono dati e informazioni a supporto delle varie attività aziendali
- Supporta le attività decisionali, di coordinamento e di controllo
- È solo l'infrastruttura tecnologica ma non le persone che contribuiscono al suo corretto funzionamento
- È in grado di guidare il personale aziendale nell'analisi dei problemi e nella visualizzazione delle possibili soluzioni
- È sempre scollegato dagli impianti produttivi
- Supporta la definizione di strategie e la conduzione esecutiva dell'azienda

(12- M3.1.1.1) Quali dei seguenti processi sono Processi Primari (processi che hanno risvolti verso l'esterno)

- Vendite e Marketing
- Organizzazione delle risorse umane
- Qualità, miglioramento dei processi e gestione dei cambiamenti
- Attività infrastrutturali (tutte le funzioni, generalmente classificate come "costi fissi")
- Supply Chain
- Gestione infrastruttura tecnologica

(13- M3.1.1.4) L'Incidente Informatico

- Può essere considerato qualsiasi evento o insieme di eventi che sottintendono una violazione delle politiche di sicurezza IT fonte di danno per gli asset IT ovvero per il patrimonio informativo

dell'organizzazione e per il quale si rende necessaria l'applicazione di misure di analisi e di contrasto e/o contenimento

- Può essere considerato qualsiasi evento che si verifichi nell'ambito di un determinato asset informatico, comunque rilevato, la cui rilevanza è considerata significativa ai fini delle attività di gestione, controllo della sicurezza e contenimento dei rischi ad essa correlati
- Può essere, ad esempio, l'accesso (logico) non autorizzato agli asset IT
- Può essere, ad esempio, la diffusione non autorizzata di informazioni riservate provenienti dagli asset IT
- Può essere, ad esempio, il tentativo di accesso (logico) ai server centrali
- Può essere ad esempio, la constatazione di illeciti o azioni criminose apportate con l'ausilio delle risorse IT

(14- M3.1.3.2) Le Procedure Operative Standard (SOP)

- Definiscono i compiti e i ruoli necessari per ottenere un risultato, nel tentativo di eliminare la dipendenza dalle singole professionalità in grado di completare specifiche attività
- Sono un insieme di documenti che offrono istruzioni esatte su come i dipendenti, i membri di un team o altri utenti in un'organizzazione o azienda devono completare un processo specifico
- Permettono la soddisfazione dei requisiti di progetto per la definizione dei nuovi investimenti
- Permettono la definizione delle buone pratiche (good practice) applicabili a una serie di azioni esplicite e dettagliate
- Permettono la definizione degli obiettivi strategici attraverso l'analisi dell'operatività
- Permettono l'assegnazione dei ruoli responsabili dell'esecuzione di ogni passaggio (ad esempio) di una lavorazione

(15- M3.2.1.2) Un Sistema di Gestione della Sicurezza delle Informazioni (SGSI o ISMS in inglese) secondo ISO/IEC 27000

- È un insieme di regole che un'azienda deve stabilire per identificare gli stakeholder e le loro aspettative nei confronti dell'azienda in termini di sicurezza delle informazioni
- È un insieme di regole che un'azienda deve stabilire per identificare gli stakeholder e le loro aspettative nei confronti dell'azienda in termini di sicurezza in generale
- È un insieme di regole per identificare quali rischi esistono specificatamente per il processo produttivo
- È un insieme di regole per definire i controlli e altri metodi di mitigazione per soddisfare le aspettative identificate e gestire i rischi
- È un insieme di regole per fissare obiettivi chiari su ciò che deve essere raggiunto con la sicurezza delle informazioni
- È un insieme di regole per attuare tutte le contromisure e gli altri metodi per il trattamento del rischio

(16- M3.2.1.5) ISO/IEC 27002 permette di strutturare in controlli secondo uno schema che prevede i seguenti livelli (indicare vero solo quelli effettivamente presenti, falso gli altri)

- ? Aree di Controllo
- ? Zone Demilitarizzate
- ? Categorie di Controllo
- ? Categorie di Rischio
- ? Impatto Possibile
- ? Contromisure (Controlli)

(17- M3.2.1.8) Quali delle seguenti sono Aree di Controllo secondo ISO 27001 2013?

- ? Acquisizione, sviluppo e manutenzione degli apparati di sicurezza
- ? Gestione degli Asset aziendali
- ? Sicurezza delle attività operative
- ? Gestione dei sistemi informativi
- ? Aspetti di sicurezza per la gestione della Business Continuity
- ? Gestione degli incidenti relativi alla sicurezza delle informazioni

(18- M3.2.3.2) Nel NIST CSF il Framework Core

- ? È un insieme di attività di sicurezza informatica, risultati desiderati e riferimenti applicabili comuni a tutti i settori delle infrastrutture critiche
- ? Presenta standard, linee guida e pratiche del settore che consentono la comunicazione di attività e risultati inerenti alla sicurezza informatica in tutta l'organizzazione dal livello manageriale sino a livello dell'implementazione e delle operations
- ? È costituito da cinque funzioni concorrenti e continue: Identifica, Proteggi, Rileva, Rispondi, Recupera
- ? È costituito da quattro funzioni concorrenti e continue: Identifica, Proteggi, Rileva, Rispondi
- ? Identifica le categorie e le sottocategorie chiave sottostanti per ciascuna funzione e le abbina a riferimenti informativi di esempio come standard, linee guida e pratiche esistenti per ciascuna sottocategoria
- ? Identifica le categorie e le abbina direttamente ai riferimenti informativi di esempio come standard, linee guida e pratiche esistenti per ciascuna sottocategoria

(19- M3.2.3.5) Nel NIST CSF i Framework Profile

- ? Possono essere visti come una fotografia dello stato corrente (o in un dato scenario di implementazione) di standard, linee guida e pratiche dell'organizzazione in relazione al Framework Core

- Possono essere utilizzati per identificare le opportunità per migliorare la posizione di sicurezza informatica confrontando un profilo "corrente" (lo stato attuale) con un profilo "target" (lo stato come lo si vorrebbe)

- Possono essere sviluppati all'interno di un'organizzazione attraverso la revisione di tutte le Categorie e Sottocategorie e, sulla base di fattori di business/missione e di una valutazione del rischio, determinare quali sono più importanti, aggiungendo Categorie e Sottocategorie e utilizzando Il profilo corrente per supportare la definizione delle priorità e la misurazione dei progressi verso il profilo target

- I Profili racchiudono al loro interno gli obiettivi organizzativi in relazione al business ma non possono in nessun modo influenzare gli investimenti aziendali

- I Profili racchiudono al loro interno la propensione al rischio dell'organizzazione in relazione alle minacce ambientali

- I Profili racchiudono al loro interno i requisiti ma non le risorse in relazione ai risultati desiderati del Core

(20- M3.2.4.1) Il NIST Special Publication 800-39

- Ha come titolo: "Managing Information Security Risk", Organization, Mission, and Information System View

- Ha come titolo: "Managing Risk in Information Security", Organization, Mission, and Information System View

- Ha come titolo: "Managing Security of Information Risk", Organization, Mission, and Information System View

- È il documento di punta della serie di standard e linee guida per la sicurezza delle informazioni sviluppati dal NIST in risposta alla FISMA (Federal Information Security Modernization Act) del Cybersecurity & Infrastructure Security Agency

- È il documento di punta della serie di standard e linee guida per la sicurezza delle informazioni sviluppati dal NIST in risposta all'FIPS (Federal Information Processing Standard) del governo degli Stati Uniti d'America

- Ha come scopo il fornire una guida per un programma ampio e integrato a livello di organizzazione per la gestione del rischio per la sicurezza delle informazioni in relazione al funzionamento e all'uso dei sistemi informativi federali degli Stati Uniti

(21- M3.2.6.2) La struttura di ISA/IEC 62443

- È costituita da quattro famiglie di standard con vari livelli di approfondimento

- È raggruppabile in quattro gruppi di standard che possono rappresentare: "Modelli", "Gestione", "Sistema" e "Componente"

- È composta dalle famiglie: "Modelli", "Gestione", "Organizzazione" e "Componente"

- È composta dalle famiglie: "General", "Policy & Procedures", "System" e "Component"

- È costituita da famiglie di standard con lo stesso numero di documenti in ogni famiglia

- È costituita da famiglie di standard con vari documenti in diversi stadi di sviluppo

(22- M3.2.6.5) I conduits secondo ISA/IEC 62443

- **Raggruppano gli elementi che consentono la comunicazione tra due zone**
- **Non possono essere usati per fare comunicare due o più zone fra di loro**
- **Forniscono funzioni di sicurezza che consentono una comunicazione sicura e permettono la coesistenza di zone con diversi livelli di sicurezza**
- **Consistono nel raggruppamento di cyber asset dedicati esclusivamente alle comunicazioni, e che condividono gli stessi requisiti di cybersecurity**
- **Possono avere sotto-conduits**
- **Possono attraversare più di una zona**

(23- M3.2.6.8) I Livelli di Sicurezza secondo ISA/IEC 62443-3-3

- **Sono quattro: Da SL1= Protezione contro violazioni casuali a SL4=Protezione contro violazioni con mezzi sofisticati, risorse estese, skill specifici e alta motivazione**
- **Rappresentano un metodo qualitativo per identificare la sicurezza in ciascuna zona**
- **Sono tre: da SL1= Protezione contro violazioni casuali a SL3=Protezione contro violazioni con mezzi sofisticati, risorse estese, skill specifici e alta motivazione**
- **Per la corretta definizione dei requisiti di sicurezza vengono declinati per ciascuno dei requisiti derivati dai requisiti di base o fondazionali**
- **Possono avere i requisiti di base più un certo numero di requisiti di rinforzo (Requirement Enhancement –RE)**
- **Hanno quattro tipologie di Livelli per la gestione continua: SL (Target), SL (Achieved), SL (Capability) e SL (Overflow)**

(24- M3.3.2.1) La Proprietà Intellettuale

- **È l'insieme di diritti legali volti ad assicurare la tutela delle creazioni della mente umana in campo scientifico, industriale e artistico**
- **Protegge invenzioni, lavori letterari e artistici, simboli, nomi, immagini e disegni mediante una registrazione su un apposito sito**
- **Concede diritti esclusivi legati alle varie forme di espressione della conoscenza, delle idee e delle opere artistiche**
- **Include i Brevetti (che proteggono le nuove idee)**
- **Include i Marchi depositati (che proteggono i simboli finalizzati a distinguere le varie aziende)**
- **Include il Diritto d'autore (che protegge le espressioni artistiche)**

(25- M3.3.3.2) La Cybersecurity e la Brand Reputation

- **Non hanno legami diretti**
- **Hanno legami stretti**
- **Hanno legami stretti perché gli incidenti di CyberSecurity comunicano inaffidabilità con immediata perdita di fiducia**
- **Hanno legami stretti perché gli incidenti di CyberSecurity comunicano scarsa qualità dei prodotti**
- **Hanno legami stretti perché gli incidenti di CyberSecurity comunicano fragilità e insicurezza**
- **Hanno legami stretti perché gli incidenti di CyberSecurity inadeguatezza tecnologica**

(26- M3.3.5.2) La Direttiva NIS (Network and Information Security) ha come obiettivo

- **Lo stabilire un framework di livello "elevato" di sicurezza delle reti e dei sistemi informativi comune a tutti i Paesi dell'Unione Europea**
- **Lo stabilire un framework di sicurezza delle reti e dei sistemi IT che permetta, la gestione dei rischi di sicurezza per tutte le aziende**
- **Lo stabilire un framework di sicurezza delle reti e dei sistemi IT che permetta, tra l'altro, la gestione dei rischi di sicurezza solo per gli operatori dei servizi essenziali e i fornitori di servizi digitali**
- **La nascita di CSIRT (Computer Security Incident Response Team) nazionali, sulla base del CERT-UE**
- **Lo stabilire un framework di sicurezza delle reti e dei sistemi IT che permetta, tra l'altro, di punire le organizzazioni cybercriminali con pene specifiche**
- **Lo stabilire un framework di sicurezza delle reti e dei sistemi IT che permetta, tra l'altro, la riduzione dell'impatto degli incidenti di cyber sicurezza**

(27- M3.3.6.2) Il Regolamento (UE) 2016/679 GDPR prevede i seguenti dati

- Dati personali: Informazioni relative a persona fisica identificata o identificabile
- Dati personali particolari (o sensibili secondo il codice privacy italiano): Dati generali relativi alla persona fisica identificata o identificabile
- Dati personali particolari (o sensibili secondo il codice privacy italiano): Dati su origine razziale o etnica, le opinioni politiche, dati genetici, biometrici o sulla salute
- Dati personali relativi a condanne penali o reati solo se autorizzati dall'interessato
- Dati personali relativi a condanne penali o reati sotto il controllo dell'autorità pubblica
- Dati personali relativi a condanne penali o reati se autorizzati dal diritto dell'Unione

(28- M3.3.6.5) Il Regolamento Europeo GDPR su Informativa e Consenso

❔ Prevede che il titolare debba fornire agli interessati, prima del trattamento, le informazioni sulle finalità e le modalità dei trattamenti operati dal titolare del trattamento

❔ Prevede che debba essere esplicitamente dato un valido consenso per la raccolta dei dati e per i propositi per i quali sono usati

❔ Prevede che se la richiesta di consenso viene inserita nell'ambito di altre dichiarazioni essa va distinta e formulata con linguaggio semplice e chiaro

❔ Prevede che la richiesta di consenso deve essere formulata con linguaggio semplice e chiaro e può essere formulata complessivamente una sola volta anche nel caso di altre dichiarazioni

❔ Non prevede particolari criteri di sicurezza o conservazione una volta autorizzati al trattamento

❔ Prevede che la condizione di validità del consenso è che le finalità per cui viene richiesto siano esplicite, legittime, adeguate e pertinenti

(29- M3.4.3.1) Il Rischio Informatico

❔ È il rischio di incorrere in perdite economico/finanziarie nonché di mettere a repentaglio la salute umana in seguito al verificarsi di eventi accidentali o di azioni dolose inerenti al sistema informatico

❔ È il rischio di mettere a repentaglio il sistema informatico, relativamente all'infrastruttura tecnologica

❔ Non è mai dovuto all'errore umano ma solo all'effetto di minacce informatiche come virus e malware

❔ Può essere dovuto a errore umano che apre la strada a virus e malware

❔ Può essere dovuto ad un evento accidentale che compromette il sistema informativo

❔ Può essere dovuto ad una azione dolosa di terzi

(30- M3.4.4.1) Il Paradigma RID (Riservatezza-Integrità-Disponibilità)

❔ Identifica le priorità della cyber security relativamente all'Information Technology

❔ Identifica le priorità della cyber security relativamente all'Information Technology e dell'Operational Technology (l'Informatica Industriale)

❔ Identifica, in ordine di importanza decrescente, i fattori Riservatezza, Integrità e Disponibilità/Accessibilità dei dati

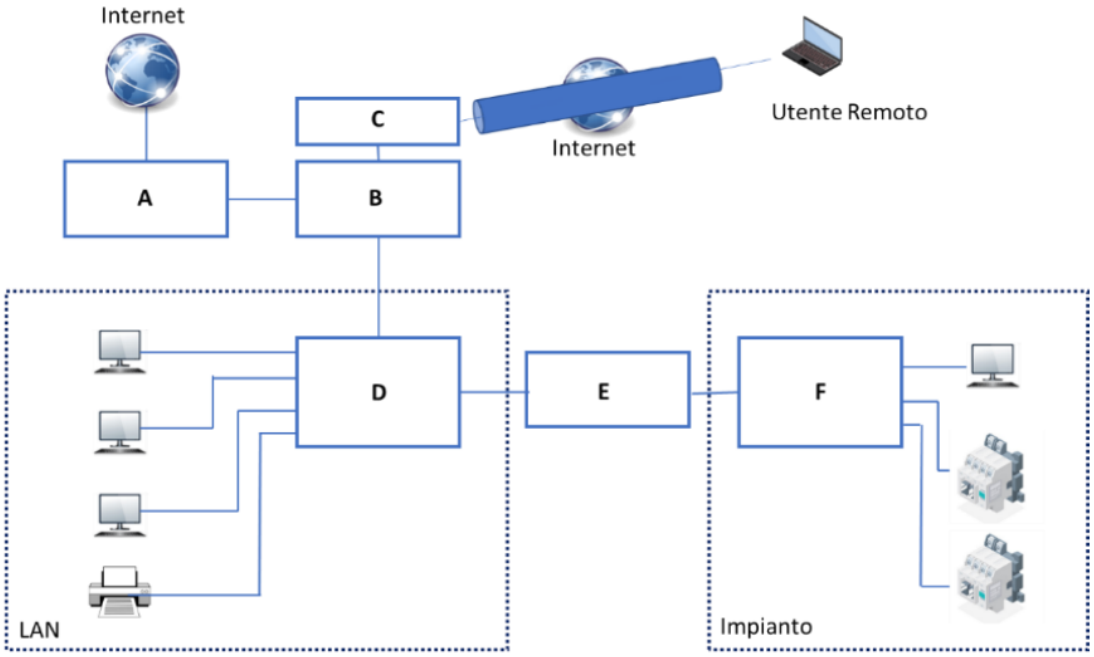
❔ Identifica, in ordine di importanza crescente, i fattori Riservatezza, Integrità e Disponibilità/Accessibilità dei dati

❔ Identifica, a parità di importanza, i fattori Riservatezza, Integrità e Disponibilità/Accessibilità dei dati

❔ Considera la Riservatezza come la necessità di impedire l'accesso non autorizzato alle informazioni sensibili

Esercizio 1:

Indicare la tipologia dei dispositivi rappresentati come rettangoli nello schema seguente (Es.: Switches, Firewall, ecc.):



A. ROUTER
B. FIREWALL
C. VPN
D. SWITCH
E. FIREWALL(Risposta corretta secondo IEC 62443), risposta accettabile SWITCH
F. SWITCH

Esercizio 2

L'amministratore di una rete aziendale con indirizzo 256.18.0.0/17 desidera: (in rosso errore mio)

- Impedire l'accesso da Internet alla rete aziendale
- Consentire l'accesso dalla rete 150.12.0.0/17 (rete locale della filiale) alla sottorete interna 256.18.21.0/24
- Impedire all'indirizzo 150.12.10.2 di poter accedere alla sottorete interna 256.18.21.0/16
- Impedire alla sottorete 150.12.20.0/26 di poter accedere alla sottorete interna 256.18.21.0/16

Configurare nella seguente tabella le regole del firewall per gestire i requisiti:

Indice	IP Sorgente (o sottorete)	IP Destinatario (o sottorete)	Azione (Blocca/Consenti)
1 (*)	150.12.20.0/26	256.18.21.0/16	Blocca
2 (*)	150.12.10.2	256.18.21.0/16	Blocca
3	150.12.0.0/17	256.18.21.0/24	Consenti
4	0.0.0.0/0	0.0.0.0/0	Blocca

(*) Si possono invertire

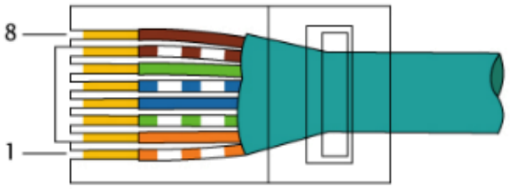
Appello 20 Giugno 2022 - T3

(1- M1.3.2.3) Lo Standard RS232

- ? Può raggiungere una velocità di trasmissione di circa 112 Kb/sec
- ? Può trasmettere sino ad una distanza massima di circa 200m
- ? Può trasmettere sino ad una distanza massima di circa 15m
- ? Può supportare sino a 2 dispositivi collegati
- ? Può supportare sino a 10 dispositivi collegati con ricevitori ad alta impedenza
- ? Ha a un cavo con tre fili

(2- M1.3.2.6) Il connettore rappresentato in figura di lato

- ? Di solito è un connettore utilizzato per connessioni di rete
- ? Ha la piedinatura RJ45
- ? Ha la piedinatura RJ11
- ? Può essere utilizzato per connessioni punto sino a 100m
- ? Può essere utilizzato per connessioni punto sino a 300m
- ? Può raggiungere velocità di 10 Gbps



EIA/TIA-568B

(3- M1.3.2.9) Nella comunicazione con il protocollo Ethernet in caso di avvenuta collisione:

- ? La stazione trasmittente sospende la trasmissione e trasmette una sequenza di jamming
- ? La stazione trasmittente sospende la trasmissione e trasmette una sequenza composta dalla parte di pacchetto già trasmessa e un codice identificativo in coda al pacchetto
- ? La stazione trasmittente sospende la trasmissione e trasmette e un codice identificativo in testa e la parte di pacchetto già trasmessa in coda al pacchetto
- ? La stazione di trasmissione, dopo l'invio della sequenza di jamming, ripete il tentativo di trasmissione dopo un tempo pseudocasuale
- ? La stazione di trasmissione, dopo l'invio della sequenza di jamming, ripete il tentativo di trasmissione con una frequenza fissa
- ? La stazione trasmittente interrompe le trasmissioni e attende sino a che tutte le trasmissioni sul bus siano ultimate

(4- M1.3.2.12) La comunicazione real-time:

- ? È una qualsiasi forma di comunicazione per cui gli utenti possono scambiarsi informazioni istantaneamente o con una latenza trascurabile o comunque predefinita
- ? È una qualsiasi forma di comunicazione per cui gli utenti possono scambiarsi informazioni nell'esatta sequenza che sono state generate anche se con una latenza non prevedibile o non predefinita

- Ha, di solito, necessità di garantire il determinismo nella comunicazione tra due o più dispostivi
- Può permette il controllo di dispositivi meccanici da remoto
- Deve garantire tempi di trasmissione sempre sotto il millisecondo
- Deve garantire tempi di trasmissione compatibili con i dispositivi o i processi coinvolti nella comunicazione

(5- M1.3.3.3) Lo switch di rete

- Se di tipo “cut-through” viene calcolato il CRC per il controllo degli errori
- È un dispositivo elettronico/elettrico non dotato di CPU
- Permette la segmentazione attraverso VLAN
- Se di tipo “unmanaged” permette la configurazione delle porte
- Può gestire funzioni dei livelli 3,4 e 7 dello stack ISO/OSI
- Se di tipo “managed” permette di duplicare le trasmissioni su canali differenti

(6- M2.1.1.1) L’Azienda:

- È un’organizzazione di persone e beni economici
- È un’organizzazione di persone e beni economici ma non beni strumentali
- È organizzata dall’imprenditore per l’esercizio delle funzioni che permettono di raggiungere gli obiettivi prefissati dell’impresa
- Ha al suo interno anche beni strumentali, ovvero beni economici utilizzati per la produzione di altri beni
- Ha al suo interno solo persone e beni materiali, ovvero che hanno consistenza fisica
- Ha al suo interno anche beni immateriali, ovvero che sono privi della materialità

(7- M2.1.2.1) Le aziende di Erogazione

- Sono aziende in cui i beni e i servizi prodotti non sono destinati allo scambio
- Sono aziende in cui i beni e i servizi prodotti sono destinati allo scambio sul mercato
- Sono aziende in cui i beni e i servizi prodotti sono destinati direttamente al soddisfacimento dei bisogni di un particolare gruppo di persone
- Sono aziende in cui i beni e i servizi prodotto sono destinati alla vendita dietro il ricevimento di un corrispettivo
- Sono aziende come le fondazioni e le corporazioni
- Possono essere pubbliche o private

(8- M2.1.2.4) Le aziende di produzione

- Hanno obiettivi primari legati alla stessa sopravvivenza dell'impresa
- Possono essere solo le aziende che assemblano direttamente i beni o forniscono direttamente i servizi
- Possono essere sia le aziende che producono direttamente beni o servizi sia quelle che creano valore aggiunto a beni e servizi già esistenti
- Hanno tra gli obiettivi la massimizzazione del profitto
- Hanno tra gli obiettivi la soddisfazione di un limitato gruppo di persone
- Non possono essere aziende individuali

(9- M2.1.3.3) Le Infrastrutture Critiche

- Non sono le Utility
- Sono elementi (delle infrastrutture pubbliche), sistemi o parte di questi che sono essenziali per il mantenimento delle funzioni vitali della società il cui danneggiamento o la cui distruzione avrebbe un impatto significativo su una Paese
- Possono erogare servizi come la trasmissione dell'energia attraverso gli elettrodotti
- In Italia e in Europa possono essere denominate OSE (Operatori di Servizi Essenziali) anche se non tutte le Utility sono negli elenchi delle OSE
- In Italia e in Europa tutte le Utility sono denominate OSE (Operatori di Servizi Essenziali)
- Basano l'attività e sono relative alla salute, la sicurezza e al benessere economico e sociale dei cittadini

(10- M2.3.1.1) La Gestione Aziendale

- È l'insieme delle operazioni soggettive di conduzione che il manager compie per raggiungere gli obiettivi prefissati
- È l'insieme coordinato di operazioni soggettive e oggettive che l'azienda compie per raggiungere gli obiettivi prefissati
- Realizza operazioni soggettive, ovvero le attività svolte dagli organi aziendali, decisioni e controlli, da effettuare al fine di raggiungere gli obiettivi fissati
- Definisce i piani strategici e organizzativi
- Realizza operazioni oggettive ovvero le attività che devono essere fatte continuativamente e concretamente per realizzare, in maniera profittevole, gli obiettivi
- Realizza operazioni oggettive e soggettive per il raggiungimento della soddisfazione del cliente

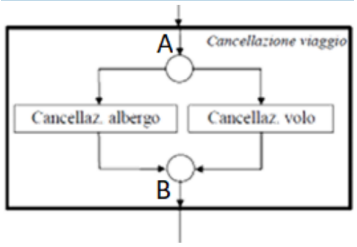
(11- M2.3.2.1) I Processi Aziendali

- Possono essere definiti come un insieme di attività, non necessariamente collegate, che possono portare a diversi obiettivi a carattere strategico
- Può essere definito come un insieme di attività collegate tese al raggiungimento di un obiettivo specifico
- Devono prevedere input, chiaramente ben definiti, e un singolo risultato finale
- Devono prevedere un solo input chiaramente definito e più risultati finali
- Hanno input che sono costituiti da tutti i fattori che contribuiscono (direttamente e indirettamente) al valore aggiunto di un servizio o di un prodotto
- I processi si possono modellizzare attraverso l'uso dei diagrammi di flusso

(12- M3.1.1.2) L'Incident Response Plan (Piano di risposta agli incidenti)

- Permette di rispondere ad un attacco esterno mediante misure controffensive verso l'attaccante
- Permette di rispondere all'esigenza di individuare gli attacchi e mitigare il danno
- Esegue anche la post analysis che consente di delineare la reale portata dell'incidente
- È un insieme di procedure documentate che descrivono in dettaglio i passaggi da intraprendere in ciascuna fase della risposta agli incidenti
- Se ben strutturato e documentato può non essere aggiornato frequentemente
- Dovrebbe includere linee guida per ruoli e responsabilità, piani di comunicazione e processi di risposta standardizzati

(13- M3.1.2.1) Nel workflow parziale WIDE rappresentato sotto



- Entrati nella Business Transaction per il punto A i task Cancellazione Albergo e Cancellazione Volo vengono eseguiti uno dopo l'altro (terminato Cancellazione Albergo viene eseguito Cancellazione Volo)
- Entrati nella Business Transaction per il punto A i task Cancellazione Albergo e Cancellazione Volo vengono eseguiti contemporaneamente
- Si giunge al punto B solo dopo che almeno uno tra i task Cancellazione Albergo e Cancellazione Volo è stato eseguito completamente
- Si giunge al punto B solo dopo che entrambi i task Cancellazione Albergo e Cancellazione Volo sono stati eseguiti completamente

? Si giunge al punto B anche se nessuno tra i task Cancellazione Albergo e Cancellazione Volo è stato eseguito completamente

? Si giunge al punto B solo se i task Cancellazione Albergo e Cancellazione Volo si concludono contemporaneamente

(14- M3.1.3.3) La certificazione aziendale

? È la dichiarazione di un ente indipendente o accreditato che il prodotto fornito o le politiche messe in atto dall'azienda sono conformi ad una certa normativa o standard di riferimento

? È la dichiarazione di un ente indipendente o accreditato che si formalizza attraverso l'emissione di un certificato con validità illimitata

? È la dichiarazione di un ente terzo che il prodotto fornito o le politiche messe in atto dall'azienda sono conformi ad una certa normativa o standard di riferimento

? Se di sistema, permette di stabilire un meccanismo continuo di verifica della conformità ad uno standard ed il miglioramento continuo di un sistema di gestione

? Se di sistema, permette di stabilire un meccanismo di verifica puntuale della conformità ad uno standard ma non permette la verifica periodica del sistema di gestione

? Può essere uno strumento per rispondere alle richieste sempre più pressanti del mercato per differenziarsi dai competitors ed entrare, in nuovi mercati, mai esplorati prima

(15- M3.2.1.3) Quale di queste aree non è un requisito di un ISMS ISO 27000

? Contesto dell'Organizzazione

? Leadership

? Pianificazione

? Supporto

? Business Continuity

? Data Security

(16- M3.2.1.6) Quali delle seguenti sono Aree di Controllo secondo ISO 27001 2013?

? Politiche per la sicurezza delle informazioni

? Organizzazione della sicurezza delle informazioni

? Sicurezza del personale

? Gestione dell'infrastruttura di rete

? Controllo degli accessi "fisici" ai sistemi, agli asset e gli apparati

? Crittografia

(17- M3.2.1.9) Secondo ISO 27002 2013 un Obiettivo di Controllo è

- È la dichiarazione di cosa si vuole raggiungere
- È il controllo stesso
- È la descrizione estesa della finalità dello specifico controllo
- È di fatto la Categoria del Controllo
- È l'appropriata contromisura in esame
- Nessuno dei precedenti

(18- M3.2.3.3) Nel Framework Core (di NIST CSF) le Categorie

- Sono le suddivisioni di ciascuna delle Funzioni Concorrenti in gruppi di possibili fattori di rischio di sicurezza informatica legati alle esigenze programmatiche e ad attività generiche
- Sono le suddivisioni di ciascuna delle Funzioni Concorrenti in gruppi di risultati di sicurezza informatica strettamente legati alle esigenze programmatiche e ad attività particolari
- Possono includere, ad esempio, "Gestione degli asset", "Gestione dell'identità e controllo degli accessi" e "Processi di rilevamento"
- Sono ulteriormente suddivise in sottocategorie le quali forniscono una serie di risultati che, sebbene non esaustivi, aiutano a supportare il raggiungimento degli obiettivi (risultati o outcomes) in ciascuna categoria
- Sono ulteriormente suddivise in sottocategorie che possono includere, ad esempio, "I sistemi di informazione esterni sono catalogati", "I dati inattivi sono protetti" o "Le notifiche dai sistemi di rilevamento vengono esaminate"
- Sono ulteriormente suddivise in sottocategorie che sono associate a Riferimenti Informativi: esempi assolutamente esaustivi basati sulle esperienze dirette sul campo

(19- M3.2.3.6) Nel NIST CSF il Coordinamento dell'implementazione del Framework

- Il livello esecutivo (A) comunica le priorità della missione, le risorse disponibili e la tolleranza complessiva al rischio al livello di business/processo (B)
- Il livello aziendale di business/processo (B) utilizza le informazioni come input nel processo di gestione del rischio; quindi, collabora con il livello di implementazione/operativo (C) per comunicare le esigenze aziendali e creare un profilo
- Il livello di implementazione/operativo (C) comunica l'avanzamento dell'implementazione del Profilo al livello di business/processo (B)
- Il livello aziendale/di processo (B) utilizza queste informazioni (Domanda 3) per eseguire una valutazione d'impatto
- La gestione del livello business/processo (B) riporta i risultati di tale valutazione d'impatto (Domanda 4) al livello esecutivo (A) per informare il processo complessivo di gestione del rischio dell'organizzazione e al livello di implementazione/operativo (C) per le modifiche al processo

(20- M3.2.4.2) NIST Special Publication 800-53 Rev. 5

- Fornisce un catalogo di controlli di sicurezza e privacy per i sistemi informativi e le organizzazioni per proteggere le operazioni e le risorse organizzative, gli individui, le aziende e la nazione da una serie diversificata di minacce e rischi di varia natura
- Fornisce un catalogo di controlli di sicurezza e privacy per i sistemi informativi e le aziende per proteggere le operations e le risorse organizzative, gli individui, le aziende e la nazione da minacce e rischi di varia natura
- Sono un catalogo di controlli, ovvero contromisure, estratti direttamente e senza variazioni dal FISMA (Federal Information Security Modernization Act)
- Ha come titolo: “Security and Privacy Controls for Information Systems and Organizations”
- Ha come titolo: “Security Controls for Information Systems and Organizations”
- Ha come titolo: “Security and Privacy Controls for the Government Information Systems”

(21- M3.2.6.3) In un CSMS secondo ISA/IEC 62443

- I requisiti sono associati agli elementi costitutivi raggruppati in macrocategorie
- Le macrocategorie sono: “Risk Analysis”, “Indirizzare il rischio con il CSMS”, “Monitorare e migliorare il CSMS”
- Ad ogni elemento è associato un elenco di requisiti specifici
- Ad ogni elemento è associato solo un requisito specifico
- Gli elementi non sono ulteriormente raggruppati all’interno delle macrocategorie
- Per ciascun elemento sono rappresentati gli obiettivi, la descrizione e il fondamento logico (rationale) dell’elemento

(22- M3.2.6.6) I Foundational Requirements secondo ISA/IEC 62443

- Sono stati definiti dal momento che il classico modello CIA (Confidentiality, Integrity e Availability) non assicura una completa comprensione dei requisiti pe34r gli IACS (Industrial Automation and Control Systems)
- Sono stati definiti dal momento che il classico modello CIA (Confidentiality, Integrity e Availability) non assicura una completa comprensione dei requisiti per gli apparati di rete
- Sono sette requisiti di base
- Sono quattordici requisiti di base
- Sono otto requisiti di base
- Focalizzano gli aspetti di cyber sicurezza in relazione al funzionamento degli IACS

(23- M3.2.6.9) I Maturity Level secondo ISA/IEC 62443-4-1

- Sono 4 livelli di maturità dei fornitori di componenti (prodotti) da un livello “Iniziale” (1) ad un livello quantitativamente gestito o di “Miglioramento” (4)
- Sono 3 livelli di maturità dei fornitori di componenti (prodotti) da un livello “Iniziale” (1) ad un livello quantitativamente gestito o di “Miglioramento” (3)
- Sono 4 livelli di maturità dei fornitori di sistemi da un livello “Iniziale” (1) ad un livello quantitativamente gestito o di “Miglioramento” (4)
- Identificano i processi di sviluppo del prodotto in termini di documentazione, ripetibilità e controllo dei processi, skill del personale
- Identificano i processi di sviluppo del prodotto e dei sistemi in termini di documentazione, ripetibilità e controllo dei processi, skill del personale
- Hanno livelli intermedi di tipo; “Gestito” con processi codificati e ripetibili e “Definito” in cui ci sono anche evidenze che i processi siano praticati.

(24- M3.3.2.2) Si può brevettare

- Un’invenzione se si tratta di una “soluzione nuova e originale ad un problema tecnico”, che rappresenti cioè un risultato dell’ingegno umano e del progresso tecnico
- Un’invenzione se si tratta di una “soluzione nuova e originale ad un problema tecnico o scientifico”, che rappresenti cioè un risultato dell’ingegno umano e della ricerca tecnica o scientifica
- Un’invenzione se ha requisito di “Novità”: L’invenzione è nuova se non è compresa nello stato della tecnica alla data di richiesta di brevetto
- Un’invenzione se è il risultato di “Attività inventiva”: L’invenzione implica attività inventiva solo se ha caratteristiche di originalità per un esperto del settore, non sono sufficienti quindi unicamente le caratteristiche di novità ma la novità non deve essere «banale» o «ovvia»
- Un’invenzione anche se contraria all’ordine pubblico e al buon costume ma che abbia caratteristiche innovative
- Un’invenzione se ha requisito di “Industrialità “: Oggetto del brevetto di pertinenza di aziende industriali

(25- M3.3.4.1) L’Informatica Forense

- È la disciplina che studia l’insieme delle attività che sono rivolte all’analisi e alla soluzione dei casi legati alla criminalità informatica
- Comprende i crimini realizzati con l’uso di un computer, diretti a un computer o in cui il computer può comunque rappresentare una fonte di prova
- Rappresenta una branca delle scienze forensi e la sua importanza è evidente solo nei casi di criminalità informatica con elevata rilevanza giuridica
- Rappresenta una branca delle scienze forensi e la sua importanza è evidente non solo nei casi di crimini informatici, ma anche nell’ambito dei processi civili

- Permette di rilevare le informazioni generate e trasmesse in formato digitale, con valore probatorio, sulle quali si può fare affidamento in tribunale
- Nei processi civili non può essere utilizzata perché i giudici non accettano il ricorso alle cosiddette prove digitali

(26- M3.3.5.3) CERT-UE secondo la Direttiva NIS

- È la squadra di pronto intervento informatico per le istituzioni, gli organi e le agenzie dell'UE
- Comprende un gruppo di esperti in sicurezza informatica provenienti dalle istituzioni e dagli organi dell'UE
- Può avere funzioni di polizia giudiziaria anche nelle giurisdizioni dei singoli paesi
- Raccoglie, gestisce, analizza e condivide informazioni con le istituzioni, gli organi e le agenzie dell'UE in merito a minacce, vulnerabilità e incidenti riguardanti le infrastrutture TIC non classificate (non segrete)
- Raccoglie, gestisce, analizza e condivide informazioni con le istituzioni, gli organi e le agenzie dell'UE in merito a minacce, vulnerabilità e incidenti riguardanti tutte le aziende
- Coordina le risposte agli incidenti a livello interistituzionale e istituzionale, ad esempio fornendo o coordinando la fornitura di assistenza operativa specializzata

(27- M3.3.6.3) Il Data Protection Officer (DPO) secondo il Regolamento (UE) 2016/679

- È una figura specificatamente introdotta dal Regolamento
- È un professionista che deve avere un ruolo aziendale (sia esso soggetto interno o esterno) con competenze giuridiche, informatiche, di risk management e di analisi dei processi
- È un professionista con competenze giuridiche, informatiche, di risk management e di analisi dei processi che deve essere un soggetto obbligatoriamente esterno rispetto all'azienda che ne chiede il servizio
- Ha la responsabilità principale di osservare, valutare e organizzare la gestione del trattamento di dati personali affinché questi siano trattati nel rispetto delle normative privacy europee e nazionali
- È una figura tecnica e giuridica, con potere esecutivo
- Di solito si appoggia al CISO che funge da tramite fra l'organizzazione e l'autorità

(28- M3.3.7.1) Enisa secondo il Regolamento (UE) 2019/881

- È l'Agenzia dell'Unione europea per la cibersicurezza, e la certificazione della cibersicurezza per le tecnologie dell'informazione e della comunicazione
- Agisce attraverso le sotto-Agenzie, dell'Agenzia stessa, che verranno create al livello di singoli Stati membri
- Ha lo scopo di conseguire un elevato livello comune di cibersicurezza in tutta l'Unione, anche sostenendo attivamente gli Stati membri, le istituzioni, gli organi e gli organismi dell'Unione nel miglioramento della cibersicurezza

? Funge da punto di riferimento per pareri e competenze in materia di cibersicurezza per le istituzioni, gli organi e gli organismi dell'Unione nonché per altri portatori di interessi pertinenti dell'Unione

? Sfrutta solo risorse esterne presenti in altre organizzazioni europee

? Non si occupa direttamente di stabilire le misure per la riconciliazione delle disposizioni legislative, regolamentari e amministrative degli Stati membri relative alla cibersicurezza

(29- M3.4.3.2) Il Rischio Informatico può essere valutato come

? Impatto / Probabilità

? Impatto x Probabilità

? Impatto – Probabilità

? Un numero compreso tra un valore minimo e uno massimo in funzione dell'incertezza del rischio

? Un numero sempre compreso tra 1 (Rischio Molto Basso) e 4 (Rischio Molto Basso Alto) in funzione dell'incertezza del rischio

? Un numero che è funzione dell'incertezza e fa riferimento a classi omogenee di eventi, per natura e gravità

(30- M3.4.5.1) Il SIEM

? E' l'acronimo di Security Information and Event Management)

? E' l'acronimo di Security Impact and Event Management)

? È una soluzione software che, in tempo reale, provvede al monitoraggio e alla gestione degli eventi e delle informazioni che accadono all'interno della rete e sui vari sistemi di sicurezza fornendo una correlazione e aggregazione tra essi

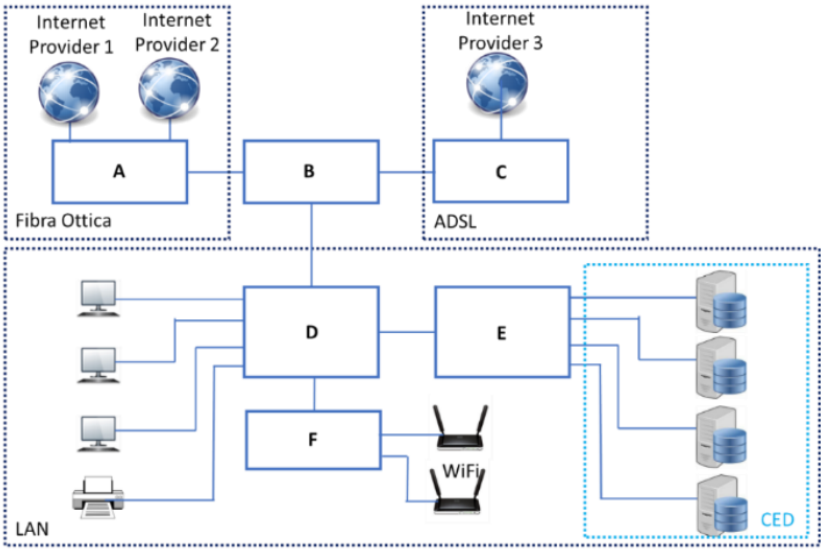
? È una soluzione software che, con una discreta latenza, provvede al monitoraggio e alla gestione degli eventi e delle informazioni che accadono all'interno della rete e sui vari sistemi di sicurezza fornendo una correlazione e aggregazione tra essi

? È una soluzione solamente hardware che provvede al monitoraggio e alla gestione degli eventi e delle informazioni che accadono all'interno della rete e sui vari sistemi di sicurezza

? Ha come interfaccia una console centralizzata, preposta ad attività di monitoraggio, segnalazione e risposta automatica a determinati eventi

Esercizio 1

Indicare la tipologia dei dispositivi rappresentati come rettangoli nello schema seguente (Es.: Switches, Firewall, ecc.):



A. ROUTER
B. FIREWALL
C. ROUTER
D. SWITCH
E. SWITCH
F. SWITCH

Esercizio 2

L'amministratore di una rete aziendale con indirizzo 256.18.0.0/17 desidera: (in rosso errore mio)

- impedire l'accesso da Internet alla rete aziendale
- consentire l'accesso dalla rete 150.12.0.0/17 (rete locale della filiale) alla sottorete interna 256.18.21.0/24
- impedire all'indirizzo 150.12.10.2 di poter accedere alla sottorete interna 256.18.21.0/16
- Impedire alla sottorete 150.12.20.0/26 di poter accedere alla sottorete interna 256.18.21.0/16

Configurare nella seguente tabella le regole del firewall per gestire i requisiti:

3	**IP Sorgente (o sottorete)**	**IP Destinatario (o sottorete)**	**Azione (Blocca/Consenti)**
1 (*)	150.12.20.0/26	256.18.21.0/16	Consenti
2 (*)	150.12.10.0/24	256.18.21.0/16	Consenti
3	150.12.0.0/17	256.18.21.0/24	Blocca
4	0.0.0.0/0	0.0.0.0/0	Blocca

(*) 1 e 2 possono essere invertiti

9 Settembre 2022 - T1

(M1.1.2.8) La banda di trasmissione VHF

- ? Identifica una banda di onde ultracorte
- ? Identifica una banda di onde ultralunghe
- ? Identifica una banda di frequenze molto elevate
- ? Ha una banda di frequenze che va da 30 a 300MHz
- ? Ha una banda di frequenze che va da 3 a 30 Ghz
- ? È utilizzata dai Radar, dai link a microonde e dalle comunicazioni satellitari

(M1.1.2.10) La quantità di informazioni che è possibile trasmettere nell'unità di tempo in un canale

- ? È inversamente proporzionale alla larghezza di banda del canale
- ? È proporzionale alla larghezza di banda del canale
- ? È maggiore al crescere dell'ampiezza dello spettro delle frequenze che possono passare per quel canale
- ? Dipende dalla tipologia del canale
- ? È indipendente dalla tipologia del canale
- ? È cresciuta largamente grazie allo sviluppo delle tecnologie elettroniche

(M1.1.3.1) Il Packet Switching

- ? È una tecnica di commutazione in cui messaggi consecutivi vengono raggruppati in pacchetti (packets) che vengono trasmessi simultaneamente
- ? È una tecnica di commutazione in cui il messaggio viene diviso in parti più piccole (packets) che vengono gestite singolarmente
- ? È una tecnica di commutazione in cui i pacchetti viaggiano attraverso la rete, prendendo il percorso più breve possibile (instradamento)
- ? È una tecnica di commutazione in cui tutti i pacchetti vengono suddivisi e trasmessi in maniera indipendente e riassemblati all'estremità ricevente nell'ordine corretto
- ? Prevede che se un messaggio arriva mancante di pacchetti o danneggiato, verrà inviata una notifica per inviare nuovamente il messaggio, se invece viene raggiunto l'ordine corretto dei pacchetti, verrà inviata notifica di conferma
- ? Prevede che se un messaggio arriva mancante di pacchetti o danneggiato il messaggio verrà considerato comunque corretto perché verrà corretto da un meccanismo di completamento automatico a correzione di errore

(M1.1.3.3) Il Routing Statico

- Può essere utilizzato anche quando il numero di dispositivi è elevato
- Può utilizzare l'algoritmo OSPF (Open Shortest Path First)
- Può utilizzare l'algoritmo RIP (Routing Information Protocol)
- Richiede l'intervento umano nella scelta delle rotte, attraverso la configurazione manuale delle rotte
- È gestito dai routers mediante la collaborazione con gli altri routers attraverso degli speciali protocolli
- Identifica i path migliori e provvedere di riempire automaticamente le tabelle di routing

(M1.1.3.4) Un indirizzo IPv6 ha la dimensione di

- 32 bits, divisi in 4 ottetti binari
- 32 bits, divisi in 8 gruppi da 4 bits
- 128 bits, divisi in 8 gruppi da 16 bits
- 128 bits, divisi in 16 gruppi da 8 bits
- 256 bits, divisi in 32 gruppi da 8 bits
- 256 bits, divisi in 8 gruppi da 32 bits

(M1.1.3.6) Il Subnetting

- È una suddivisione dello spazio di indirizzi riservato ad una rete
- È una tecnica che permette di dividere una rete in sottoreti
- È utilizzato per risolvere al problema del numero limitato degli indirizzi IP pubblici, permettendo ad ogni azienda avere a disposizione un gran numero di indirizzi IP privati
- Si realizza attraverso l'utilizzo (nella versione IPv4) della mascheratura degli ottetti binari dell'indirizzo
- Si realizza attraverso l'utilizzo (nella versione IPv4) della mascheratura dei quartetti binari dell'indirizzo
- Si realizza utilizzando una parte dei bit del prefisso di rete dell'indirizzo in maschera di sottorete

(M1.1.4.1) L'HyperText Transfer Protocol (HTTP)

- È un linguaggio di testo che consente la comunicazione tra client e server attraverso internet per recuperare tutte le risorse collegate
- È un linguaggio compilato che consente la comunicazione tra client e server attraverso internet per recuperare tutte le risorse collegate

- Ha come caratteristica peculiare che terminato lo scambio di messaggi la connessione si sgancia, rendendo il protocollo molto flessibile e dinamico
- Dispone di 5 comandi: Get, Head, Post, Put, Delete
- Dispone di 6 comandi: Get, Fetch, Head, Post, Put, Delete
- Di “default” utilizza la porta 80 per la comunicazione da client a host (server)

(M1.(M1.1.4.3) L’HyperText Markup Language (HTML)

- È un linguaggio di markup, ovvero che permette di indicare come disporre gli elementi all’interno di una pagina web
- Fornisce indicazioni sulla disposizione degli elementi attraverso degli appositi marcatori, detti tag
- Fornisce indicazioni sulla disposizione degli elementi attraverso dei marcatori che hanno la caratteristica di essere inclusi tra parentesi quadre
- Non può essere utilizzato liberamente ma bisogna riconoscere determinate royalties al W3C
- Permette di disaccoppiare la struttura logica di una pagina web (definita appunto dal markup) e la sua rappresentazione grafica, una volta che la pagina è caricata dal browser
- Fornisce le indicazioni attraverso un file binario, di solito, con estensione HTML, spesso detto “Pagina HTML“

(M1.1.4.4) Il World Wide Web (WWW)

- È un servizio che permette l’accesso a contenuti ipertestuali (legge documenti in formato ipertesto), e multimediali, sfruttando l'infrastruttura di Internet
- È un servizio che permette di visualizzare pagine web che hanno contenuti presenti solo sul server che gestisce il servizio
- È costituito da tre elementi o tecnologie fondamentali: l’URL, l’http e l’html
- Originariamente prevedeva la visualizzazione di sole pagine ipertestuali statiche
- L’evoluzione della tecnologia ha permesso di introdurre specifici software e linguaggi che permettono la realizzazione di effetti dinamici e interattivi
- Può funzionare anche senza un “Browser”

(M1.1.5.1) Il Virus Informatico

- È un frammento di codice eseguibile, anche autonomamente, da un programma ospite
- Deve appoggiarsi necessariamente ad un altro programma/eseguibile per essere attivato
- È auto-replicante, ovvero è in grado di creare la copia di sé stesso all'interno di altri file o computer senza il consenso o l'intervento di un utente
- Necessita del consenso o dell'intervento di un utente per gestire la duplicazione all’interno di altri file o computer

- È comparso per la prima volta negli anni 90
- Può essere considerato un “Worm”

(M1.1.6.2) Le vulnerabilità informatiche

- Sono malfunzionamenti, configurazioni sbagliate o semplicemente errori (bugs) presenti in un sistema che lo espongono a dei rischi
- Rendono un sistema vulnerabile ed esposto a potenziali minacce
- Sono esclusivamente relative al codice software o firmware embedded in una determinata motherboard
- Possono presentarsi all’interno del codice stesso, in una configurazione o addirittura nel processo di installazione
- Sono raggruppabili tre macro-categorie: software, protocolli e hardware
- Sono raggruppabili tre macro-categorie: software, protocolli e firmware

(M1.2.1.4) Il Cyberspazio

- Può essere considerato la quinta dimensione bellica: Terra, mare, cielo, spazio e cyberspazio
- Può essere considerato la quarta dimensione bellica: Terra, mare, cielo e cyberspazio
- Può essere il “terreno” per cyber attacchi volti ad ottenere informazioni militari riservate e strategiche (ad esempio di natura tecnologica)
- Di solito non riguarda o non è influenzato da problematiche di carattere geopolitico
- Può essere il “terreno” per cyber attacchi finalizzati a limitare o ad ostacolare l’accessibilità al web
- Può essere il “terreno” per cyber attacchi che minacciano l’integrità di programmi ed informazioni mettendo a repentaglio la vita di diverse persone e di minacciare gli interessi nazionali di un paese

(M1.2.2.2) Le organizzazioni Cyber «Criminali»

- Possono essere tre tipologie di organizzazioni: sovvenzionate da Governi (più o meno «canaglia»), a scopo di Lucro, oppure organizzazioni “hacktiviste”
- Possono essere quattro tipologie di organizzazioni: sovvenzionate da Governi (più o meno «canaglia»), a scopo di Lucro, “hacktiviste” oppure organizzazioni “ethical”
- Se sovvenzionate dai governi hanno come obiettivo lo sviluppo e il test di vere e proprie armi di natura cyber
- A scopo di lucro sono organizzate come vere e proprie organizzazioni mafiose, utilizzano società terze per riciclare il denaro proveniente dalle attività illecite
- A scopo di lucro utilizzano criptovalute perché non è possibile tracciare transazioni effettuate
- Utilizzano massimamente il deep and dark web ma non sembrano esserci “specializzazioni” nei vari stati o aree geografiche

(M1.2.3.4) La Supply Chain o catena di fornitura

- ? Può essere il bersaglio per un attacco indiretto ad un determinato obiettivo
- ? Permette attacchi di più difficile individuazione e, di solito, di più semplice realizzazione
- ? Può essere il bersaglio di Cyber Attacchi di solito nelle PMI (Piccole e Medie Aziende)
- ? Può essere il bersaglio di Cyber Attacchi di solito nelle Grandi Aziende
- ? Non è a rischio di Cyber Attacchi solamente se elimina l'integrazione informatica cliente-fornitore
- ? Riduce il rischio di Cyber Attacchi se implementa una corretta politica di gestione dei fornitori, ad esempio, richiedendo specifici requisiti di sicurezza informatica

(M1.3.1.13) A cosa serve il modello ISO/OSI?

- ? Il modello è stato adottato per far fronte ad una crescente necessità di standardizzazione
- ? Per risolvere il problema delle reti di computer chiuse, ovvero in grado di comunicare solo con apparati dello stesso produttore o dello stesso "brand"
- ? Per rendere indipendenti il mezzo fisico di trasmissione dal livello logico
- ? Per vincolare maggiormente il mezzo fisico al livello logico
- ? Per realizzare una comunicazione multilivello, che permetta di scegliere e adattare protocolli di comunicazione e relativi algoritmi di elaborazione alla particolare rete di telecomunicazione che si intende creare
- ? Per realizzare una comunicazione multilivello, che permetta di utilizzare lo stesso tipo di protocollo di comunicazione e relativo algoritmo di elaborazione per tutti i livelli dello stack

(M1.3.1.14) Quali di questi livelli ISO/OSI sono livelli logici legati agli Host

- ? Livello 2 – Collegamento
- ? Livello 3 – Rete
- ? Livello 4 – Trasporto
- ? Livello 5 – Sessione
- ? Livello 6 – Presentazione
- ? Livello 7 – Applicazione

(M1.3.1.16) Quali delle seguenti funzioni appartengono al livello ISO/OSI di Rete (3)

- ? Correggere gli errori mediante ritrasmissione
- ? Incapsulamento del Pacchetto
- ? Gestione Errore e Diagnostica
- ? Frammentazione e Riassemblaggio

- Gestione delle Connessioni
- Servizio orientato alla connessione

(M1.3.1.17) Quali delle seguenti funzioni appartengono al livello ISO/OSI di Trasporto (4)

- Servizio orientato alla connessione
- Corretto ordine di consegna
- Trasferimento affidabile
- Controllo di flusso
- Controllo di congestione
- Definizione della sessione

(M1.3.1.20) Cosa sono gli "Open System"?

- Sono sistemi che pur avendo sistemi operativi differenti riescono ad interagire tra loro grazie a standard predefiniti
- Sono sistemi che avendo gli stessi sistemi operativi ma hardware differenti riescono ad interagire tra loro grazie a standard predefiniti
- Sono sistemi aperti che hanno come elemento che gli accomuna il sistema operativo UNIX
- Sono gli elementi chiave alla base della standardizzazione effettuata da ISO per la comunicazione delle reti di calcolatori
- Sono gli elementi chiave dell'operazione di standardizzazione OSI (Open System Interconnection) di ISO
- Hanno permesso allo standard ISO/OSI di diventare uno standard "de facto" grazie anche all'approccio pragmatico dell'insieme di protocolli TCP/IP

(M1.3.2.13) Le Fibre Ottiche multimodali

- Prevedono una sola modalità di propagazione: un'unica lunghezza d'onda della luce nel nucleo della fibra
- Prevedono nuclei di due dimensioni e almeno cinque varianti
- Ha una distanza massima di trasmissione molto maggiore rispetto alla fibra monomodale
- Si utilizza maggiormente nelle connessioni a breve raggio
- Ha un nucleo di diametro esteso per consentire il passaggio della luce a diverse frequenze o lunghezze d'onda, in modo da trasmettere simultaneamente più canali di dati
- Ha un nucleo di vetro di dimensioni maggiori o uguali a 50 micron

(M1.3.4.1) La rete LAN (Local Area Network)

- Collega assieme più computer per un uso privato come per uso aziendale senza vincoli sul numero di connessioni
- Utilizza uno standard ampiamente e uniformemente diffuso ovvero l'Ethernet
- Utilizza per la trasmissione dati cavi in rame, o fibra ottica
- Ha una portata che dipende dagli standard e dal mezzo di trasmissione utilizzati; tuttavia, è possibile aumentarla attraverso un ripetitore (repeater)
- Con lo standard Ethernet Gigabit (100 Mbit/s), tramite cavo di rame, è possibile ottenere un raggio d'azione di diversi chilometri
- Di solito si estende per più complessi edilizi, sino ad interi quartieri

(M1.3.4.3) Quali delle seguenti sono Topologie di Rete

- Stella
- Maglia Parziale
- Maglia Completa
- Catena
- Bus
- Foglia

(M1.3.4.4) In un sistema informatico il SPOF (Single Point of Failure)

- È una parte del sistema hardware il cui malfunzionamento può portare ad anomalie o alla cessazione del servizio di tutto il sistema
- È una parte del sistema, hardware o software, il cui malfunzionamento può portare ad anomalie o alla cessazione del servizio di tutto il sistema
- È particolarmente critico nei sistemi che devono essere costantemente attivi
- Può essere evitato attraverso l'uso di componenti ridondanti, considerando che anche uno solo punto di vulnerabilità può compromettere un intero sistema
- Può essere evitato migliorando l'affidabilità dei componenti singoli
- Può riguardare anche un servizio acquisito esternamente

(M1.3.4.5) In un sistema informatico la Ridondanza

- È l'esistenza di più componenti o dispositivi dedicati ad una specifica funzione, organizzati in modo da evitare che un problema riguardante uno solo di essi determini il malfunzionamento generale dell'intero sistema
- È uno strumento fondamentale, nelle fasi progettazione e di revisione di un'architettura o una topologia di rete, per aumentare l'affidabilità e la disponibilità complessiva dei sistemi

- Deve essere realizzata affiancando componenti o dispositivi rigorosamente dello stesso tipo
- Deve essere realizzata affiancando componenti o dispositivi che realizzino le stesse funzioni nello stesso modo
- È necessario che sia presente su tutta la catena dei dispositivi (end-to-end), evitando accuratamente gli SPOF
- Può essere realizzata solamente su una parte della catena dei dispositivi

(M2.1.1.4) L'Azienda: (RIPETUTA)

- È un organismo composto di persone e beni economici, diretto al raggiungimento di un fine economico, di interesse sia pubblico sia privato
- È costituita di persone e beni economici ovvero quei beni ottenibili mediante l'attività umana o disponibili in quantità limitata
- È valutata anche in base ai marchi e i brevetti di proprietà, due tipici esempi di beni materiali
- È organizzata dall'imprenditore per l'esercizio delle funzioni aziendali che permettono sempre di massimizzare il profitto
- Ha al suo interno anche beni strumentali, ad esempio: attrezzature, impianti, marchi, brevetti
- Realizza la sua attività grazie alle funzioni aziendali ed è parte integrante della supply-chain

(M2.1.2.5) Le aziende di produzione indiretta

- Creano un valore aggiunto a beni e servizi già esistenti mediante un processo di trasformazione economica e di valorizzazione che ne aumenta l'utilità finale o ne agevola lo scambio
- Producono beni e servizi mediante un processo di produzione materiale
- Possono essere imprese bancarie, assicuratrici, commerciali ecc.
- Possono essere industrie manifatturiere, imprese agricole, ecc
- Possono essere aziende di trasporto
- Sono aziende il cui sia il soggetto giuridico che quello economico sono solo di diritto privato

(M2.1.2.6) Le aziende di produzione hanno obiettivi

- Primari ovvero legati alla stessa sopravvivenza dell'impresa
- Primari che sono collegati ai processi produttivi e alla vendita dei prodotti sul mercato
- Secondari ovvero obiettivi di importanza secondaria
- Secondari ovvero il cui raggiungimento permette di conseguire, nel modo più economico possibile, gli obiettivi primari
- Collaterali ovvero obiettivi economici come il rendimento e la massimizzazione del profitto
- Collaterali ovvero obiettivi incidentali, non previsti preventivamente

(M2.1.2.7) Le società di capitali

- ? Per legge hanno un importo minimo per il capitale sociale
- ? Per legge non hanno un importo minimo per il capitale sociale
- ? Se di piccole-medie dimensioni e con pochi soci coinvolti nell'attività sono S.r.l
- ? Prevedono più organi sociali ognuno con le proprie competenze
- ? In linea generale hanno un amministratore unico o un consiglio di amministrazione
- ? Hanno autonomia patrimoniale imperfetta: i creditori sociali possono agire sul patrimonio personale dei singoli soci ma solo dopo aver escusso infruttuosamente sul patrimonio sociale

(M2.1.3.4) Quali dei seguenti sono Macrosettori di attività delle aziende di produzione

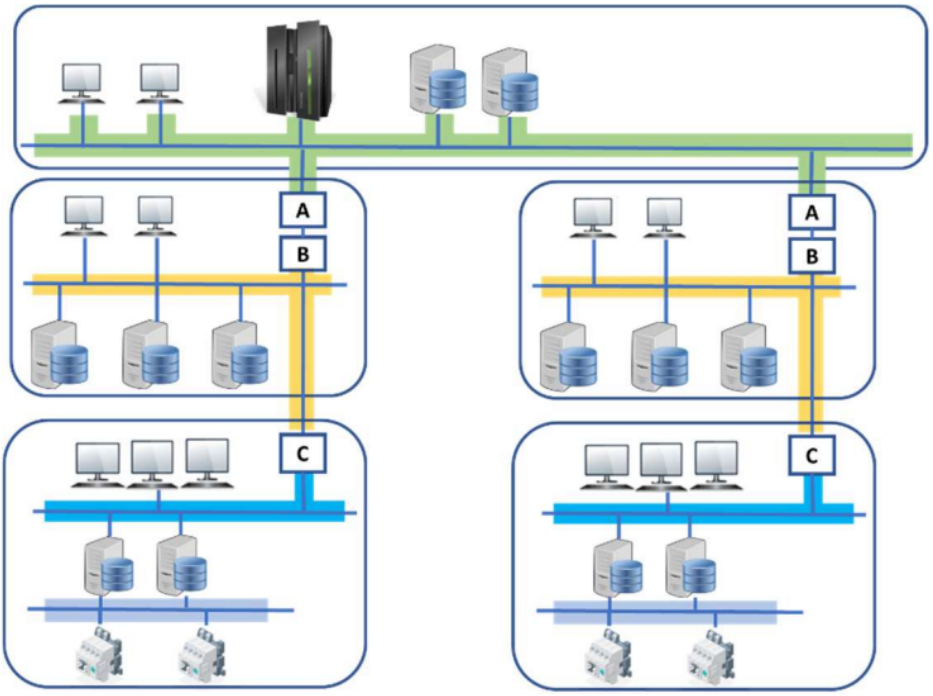
- ? Primario
- ? Produttivo diretto o Secondario
- ? Secondario avanzato
- ? Dei servizi o Terziario
- ? Terziario avanzato o Quaternario
- ? Quinario

(M2.2.1.2) Quali dei seguenti possono essere considerati asset aziendali

- ? Sistemi informativi Gestionali (Contabilità, Bilancio, Tesoreria, Cassa, Controllo di Gestione)
- ? Conoscenza commerciale: clienti, storico degli ordini, pagamenti & insoluti
- ? Impianti produttivi
- ? Facility produttivi in affitto
- ? Know-how aziendale
- ? Brevetti

Esercizio 2

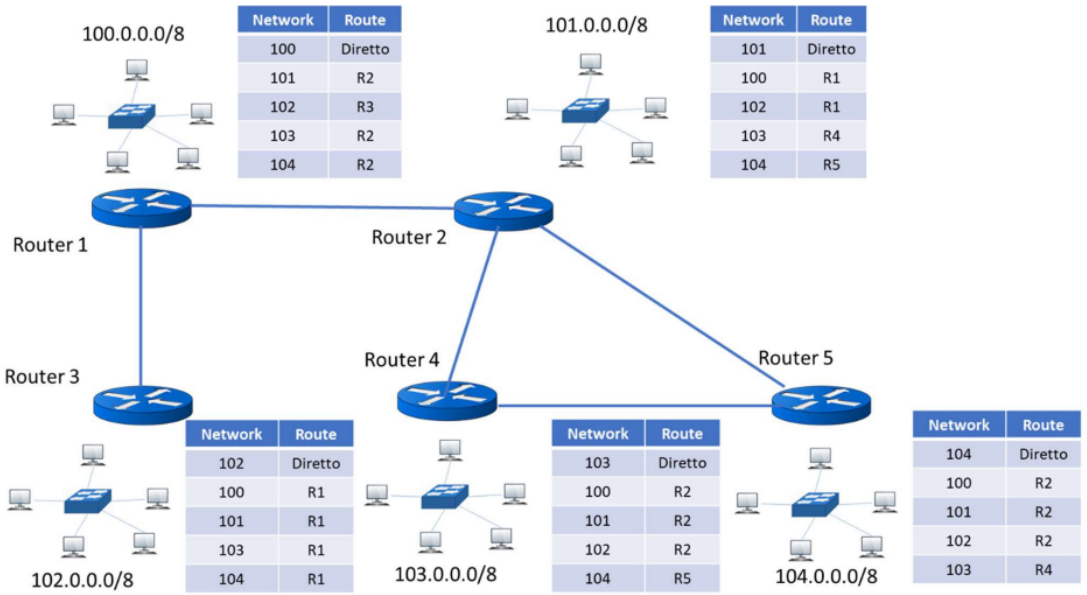
Nello schema rappresentato in figura:



1. Indicare la tipologia del dispositivo A (**Router**)
2. Indicare la tipologia del dispositivo B (**Firewall**)
3. Indicare la tipologia del dispositivo C (**Firewall**)
4. Secondo ISA/IEC 62443 come sono denominate le aree circoscritte in blu **Zone**
5. Secondo ISA/IEC 62443 come sono denominati i tratti di rete colorati in verde, giallo **Conduits**
6. Secondo ISA/IEC 62443 come sono denominati i tratti di rete colorati in azzurro e blu **Conduit**

Esercizio 2

Definire le mappe di routing del seguente schema di rete:



Nota di Dario Pedroni:

Si può notare come alcuni percorsi sono diretti, mentre altri vanno da router a router.

Esempio: **Router 1** -> **Router 5** c'è di mezzo il **Router 2** che fa da intermediario.

Appello 20 giugno 2022 - T4

(M1.3.1.12.1) L'incapsulamento ISO/OSI

❔ Introduce un "Header" con le stesse informazioni per ogni livello ISO/OSI

❔ Introduce un "Trailer" (ovvero una "coda" aggiunta al pacchetto) specifica per ogni livello ISO/OSI

❔ Introduce un "Header" (ovvero un'"intestazione" iniziale aggiunta al pacchetto) specifica per ogni livello ISO/OSI

❔ Introduce un "Header" per ogni livello e un "Trailer" (una "coda" informativa aggiunta al pacchetto) solo a livello 2

❔ Il "Trailer" di livello 2 è utilizzato per il controllo degli errori

❔ L'Header introduce le informazioni e i riferimenti necessari a ciascuno dei livelli ISO/OSI

(M1.3.2.9.1) Nella comunicazione con il protocollo Ethernet in caso di avvenuta collisione (RIPETUTA)

❔ La stazione trasmittente sospende la trasmissione e trasmette una sequenza composta dalla parte di pacchetto già trasmessa e un codice identificativo in coda al pacchetto

❔ La stazione trasmittente sospende la trasmissione e trasmette una sequenza denominata "jamming"

❔ La stazione trasmittente sospende la trasmissione e trasmette e un codice identificativo in testa e la parte di pacchetto già trasmessa in coda al pacchetto

❔ La stazione trasmittente interrompe le trasmissioni e attende sino a quando un nodo in rete inizia a ritrasmettere

❔ La stazione di trasmissione, dopo l'invio della sequenza di jamming, ripete il tentativo di trasmissione dopo un tempo pseudocasuale

❔ La stazione di trasmissione, dopo l'invio della sequenza di jamming, ripete il tentativo di trasmissione dopo un tempo prefissato

(M1.3.3.3.1) Lo switch di rete (PARZIALMENTE RIPETUTA)

❔ Può essere virtualizzato

❔ Se di tipo "cut-through" viene calcolato il CRC per il controllo degli errori

❔ Può avere una latenza non sempre trascurabile (compatibilmente con le applicazioni)

❔ Se di tipo "unmanaged" permette la configurazione delle porte

❔ Può gestire funzioni dei livelli 3,4 e 7 dello stack ISO/OSI

❔ Se di tipo "managed" permette di duplicare le trasmissioni su canali differenti (mirroring)

(M2.1.2.2.1) Il Soggetto Giuridico

❔ È il soggetto giuridicamente responsabile dell'attività svolta

❔ È la persona alla quale sono riferiti i diritti e gli obblighi che nascono dalla costituzione dell'azienda e dal suo esercizio

❔ È la persona che investe nel capitale privato dell'azienda

❔ Può essere una Persona Giuridica ovvero un ente, un'azienda o una società

❔ Può essere indifferentemente la Persona Fisica o Giuridica, entrambe hanno capacità giuridica

❔ Può essere solo una Persona Fisica nel cui nome l'attività aziendale è esercitata

(M3.2.1.3.1) Quale di queste aree non è un requisito di un ISMS ISO 27001

❔ Leadership

❔ Pianificazione

❔ Attività operative

❔ Disaster Recovery

❔ Supporto

❔ Data Entry

(M3.2.1.10) Il ciclo PDCA

❔ È il ciclo Plan Do Check Act detto anche ciclo di Deming o ciclo di Shewhart

❔ È il ciclo Process Do Control Alert detto anche ciclo di Deming o ciclo di Shewhart

❔ È un approccio al miglioramento continuo dei processi aziendali

❔ È esplicitamente indicato in ambito ISO 27000 per rappresentare il meccanismo ciclico di monitoraggio e miglioramento del sistema di gestione

❔ È esplicitamente indicato in ambito ISO 27000 per monitorare i cicli di manutenzione programmata dei sistemi

❔ Non è esplicitamente indicato in ambito ISO 27000 ma tutto lo standard è ispirato ad esso

(M3.2.6.4.1) Le zone secondo ISA/IEC

❔ Dividono un sistema in aree omogenee raggruppando le risorse (logiche o fisiche) con requisiti di sicurezza comuni

❔ Dividono un sistema in aree omogenee raggruppando le risorse fisiche con requisiti di sicurezza comuni

❔ Possono includere indifferentemente impianti presenti in uno stesso sito o in differenti locazioni geografiche

❔ Hanno requisiti di sicurezza definiti da Security Level (SL), il livello richiesto per una zona è determinato dall'analisi del rischio

❔ Hanno confini che separano gli elementi fisici da quelli virtualizzati

❔ Possono essere suddivise in sottozone che definiscono diversi livelli di sicurezza e quindi consentono una difesa in profondità

(M3.3.3.1.1) La Brand Reputation

❔ Si riferisce al modo in cui il brand o il marchio viene valutato da parte del pubblico

❔ È detta anche Brand Image ovvero la reale percezione del marchio da parte del pubblico

❔ Deve essere differenziata dalla Brand Image che risulta costruita dall’azienda in maniera strategica e può non corrispondere alla reale percezione del pubblico

❔ Può essere migliorata migliorando i contenuti pubblicati e con buone recensioni on-line

❔ Impatta direttamente l’immagine dell’azienda proprietaria del marchio

❔ Può non impattare direttamente l’immagine dell’azienda proprietaria del marchio

(M3.4.5.1.1) Il SIEM (PARZIALMENTE RIPETUTO)

❔ E’ l’acronimo di Security Impact and Event Management)

❔ E’ l’acronimo di Security Integrated and Evaluation Management)

❔ È una soluzione software che, in tempo reale, provvede al monitoraggio e alla gestione degli eventi e delle informazioni che accadono all'interno della rete e sui vari sistemi di sicurezza fornendo una correlazione e aggregazione tra ess

❔ È una soluzione software offline che provvede alla visualizzazione e alla gestione degli eventi e delle informazioni che accadono all'interno della rete e sui vari sistemi di sicurezza fornendo una correlazione e aggregazione tra essi

❔ Include le funzionalità offerte dai SIM (security information management) a quelle dei SEM (security event management)

❔ Ha come interfaccia una console centralizzata, preposta ad attività di monitoraggio, segnalazione e risposta automatica a determinati eventi

(M3.4.5.3) VPN

❔ È l'acronimo di Virtual Private Network

❔ È l'acronimo di Verified Private Network

❔ È una tecnologia che si realizza attraverso un canale di comunicazione criptato (o tunnel VPN)

❔ Consente di creare una rete privata virtuale

❔ Per il suo funzionamento può usare i protocolli IPSec (Internet Protocol Security)

❔ Per il suo funzionamento può usare i protocolli Modbus

(M3.4.5.5) Gli Instrusion Detection/Prevention

❔ Sono sistemi che si integrano con i Firewall per offrire una protezione più completa

❔ Sono sistemi che non si integrano con i Firewall ma che offrono lo stesso una protezione completa

❔ Vengono posizionati "a valle" del firewall (rispetto alla connessione Internet) ed analizzano i pacchetti di dati ed i comportamenti da loro generati

❔ Vengono posizionali "a monte" del firewall (rispetto alla connessione Internet) ed analizzano i pacchetti di dati ed i comportamenti da loro generati

❔ Per la rilevazione delle minacce possono usare la metodologia del "Misuse Detection"

❔ Per la rilevazione delle minacce possono usare la metodologia del "Deny Anomaly"

(M4.1.1.2) Quali tra le seguenti caratteristiche rientrano nel modello di Burocrazia secondo Max Weber

❔ Sviluppo di carriera

❔ Attività a tempo pieno

❔ Segreto di ufficio

❔ Stipendio monetario fisso

❔ Rimborso delle spese sostenute

❔ Non possesso strumenti del proprio lavoro

(M4.1.1.4) Perché organizzare l'azienda?

❔ Per pianificare, aumentare la produttività e di conseguenza fatturato e crescita

❔ Per sviluppare solo la parte dell'azienda più profittevole

❔ Per sincronizzare processi e sistemi costituiti da una parte sociale (risorse umane) e una parte tecnica (risorse economiche a supporto)

❔ Per aumentare il valore del prodotto o servizio che l'azienda offre ai propri clienti

❔ Per moderare la performance quando i costi superano i ricavi

❔ Per evitare problematiche dovute alla mancata collaborazione, integrazione o coordinamento di dipartimenti e risorse

(M4.1.1.6) Quali di questi sono principi fondamentali di organizzazione aziendale (indicare vero)

❔ Definire chiaramente indicatori di performance per misurazione

❔ Scegliere e creare gli strumenti di controllo di gestione adeguati come l'organigramma, il mansionario aziendale e i cruscotti aziendali

❔ Gestire il flusso d'informazioni e la comunicazione interna

❔ Lasciare l'iniziativa ai singoli

❔ Informare massimamente e primariamente solo il management

❔ Gestire l'innovazione

(M4.1.1.8) Il Controllo di Gestione

❔ È il meccanismo operativo volto a guidare il management verso il conseguimento degli obiettivi stabiliti in sede di pianificazione operativa

❔ Si utilizza unicamente nelle aziende pubbliche

❔ Rileva, attraverso la misurazione di appositi indicatori, lo scostamento tra obiettivi pianificati e risultati conseguiti e informando di tali scostamenti gli organi responsabili

❔ Rileva, grazie alle fluttuazioni della pianificazione operativa, gli elementi di scostamento con gli obiettivi ipotizzati

❔ Permette che gli organi responsabili possano decidere e attuare le azioni correttive ove necessario

❔ Può essere utilizzato nelle aziende pubbliche e nelle aziende private

(M4.1.1.10) L'Organigramma

❔ Riproduce la struttura interna di un'organizzazione o un'azienda

❔ Rappresenta i dipendenti e le posizioni attraverso caselle o altre forme su vari livelli, linee dritte o a gomito collegano insieme tali livelli

❔ È una rappresentazione parziale della gerarchia e dei ranghi delle persone, delle aree funzionali o dei raggruppamenti che compongono l'organizzazione

❔ Può rappresentare strutture organizzative Funzionali

❔ Può rappresentare strutture organizzative Vettoriali

❔ Può rappresentare strutture organizzative Matriciali

(M4.1.1.12) La Struttura Organizzativa Funzionale

❔ È la soluzione organizzativa dove le attività sono divise per “specialità”, ovvero le operazioni della medesima natura sono raggruppate tra loro

❔ È la soluzione organizzativa dove le attività sono divise per “specialità”, ovvero le operazioni della medesima natura sono raggruppate per area geografica

❔ Ha come vantaggio l’incremento dell’efficienza della direzione poiché i manager possono concentrare la loro attività in un solo settore di attività

❔ Ha come svantaggio il minore coordinamento all’interno della funzione a causa dell’assegnazione del potere decisionale ad un solo general manager per tutte le funzioni

❔ Ha come vantaggio la moltiplicazione dei livelli gerarchici, rendendo più semplice il coordinamento tra le funzioni

❔ Ha come rischio l’eccessiva focalizzazione da parte del manager sulla propria funzione, dandole eccessiva rilevanza rispetto alle altre attività aziendali

(M4.1.1.16) La Struttura Organizzativa a Matrice

❔ Presenta responsabili distinti per funzioni e per prodotti / progetti

❔ Presenta un manager di funzione per l’allocazione delle risorse a ciascun progetto (finanziamenti, impianti, ecc.) e un manager con la responsabilità della conduzione e dei risultati dei singoli prodotti/progetti

❔ Presenta una minore chiarezza dei ruoli nel processo decisionale rispetto alle altre strutture

❔ Presenta una maggiore efficienza e velocità nella comunicazione e nelle decisioni

❔ Presenta maggiori possibilità di conflitti (alle intersezioni delle linee) poiché esistono due manager allo stesso livello con lo stesso grado di autorità

❔ Permette una maggiore acquisizione di “potere” da parte di chi riesce a risolvere i conflitti, pur non ricoprendo il ruolo di responsabile

(M4.1.3.1) La figura del CISO (Chief Information Security Officer)

❔ Ha responsabilità diretta sulla sicurezza fisica delle persone

❔ Ha responsabilità diretta sulla Cyber Security di reti e sistemi

❔ Ha maggiore focalizzazione sulla tecnologia del DPO (Data Protection Officer)

❔ Ha minore focalizzazione sulla tecnologia del DPO (Data Protection Officer)

❔ Ha sempre una forte focalizzazione sulla protezione dei dati e delle informazioni

❔ Ha una maggiore focalizzazione sugli aspetti legali rispetto al DPO (Data Protection Officer)

(M4.1.3.3) Indicare con vero quali dei seguenti sono compiti del CIO (Chief Information Officer)

❔ Contribuire alla gestione del cambiamento in seguito all'introduzione di nuovi strumenti informativi

❔ Contribuire alla gestione del cambiamento proponendo l'introduzione di nuovi macchinari o tecnologie produttive

❔ Partecipare alla definizione della Business Impact Analysis (BIA)

❔ L'identificazione delle minacce: essere aggiornati sulle tipologie di minacce e di attacco

❔ L'investigazione forense: condurre indagini forensi in caso di incidenti, collaborando con risorse interne o specialisti esterni

❔ Assicurarsi che l'azienda sia conforme alle normative locali, nazionali e globali, in particolare in aree come la salute e la sicurezza

(M4.1.5.1) Il Security Auditor

❔ È lo specialista che ispeziona/valuta l'efficacia delle soluzioni tecniche adottate per garantire la sicurezza di un sistema informativo

❔ Può lavorare in un gruppo di auditing interno all'azienda o può essere un consulente esterno

❔ Lavora solamente come dipendente in gruppi di auditing interni all'azienda

❔ Fa uso dei principali linguaggi di programmazione

❔ Ha un'approfondita conoscenza dei software di sicurezza

❔ Ha dimestichezza in ambito data mining

(M4.1.5.3) L'Ethical Hacker

❔ È un esperto di sicurezza informatica capace di simulare, anticipare e prevenire attacchi informatici

❔ L'Ethical Hacker simula attacchi al sistema informatico dell'azienda di riferimento al fine di individuare eventuali falle

❔ È sempre un dipendente dell'azienda o dell'organizzazione che ne richiede il servizio

❔ Fa uso dei principali linguaggi di programmazione

❔ Ha conoscenza delle tecniche di Vulnerability Assessment

❔ Conosce tools e framework per la simulazione del processo industriale

(M4.2.2.1) Il Security Awareness

❔ Indica la consapevolezza del personale in relazione alla Cyber Security

- Indica la consapevolezza del personale in relazione alla sicurezza fisica (Safety) e logica
- Può essere migliorato attraverso la formazione e sensibilizzazione continua dei dipendenti per renderli consapevoli delle minacce cyber
- Può essere migliorato cercando di ridurre l'incidenza degli errori umani e i costi legati a un eventuale danno reputazionale
- Può essere migliorato attraverso l'educazione dei fornitori e dei clienti in merito alle policy e procedure già definite dall'organizzazione ma che non vengono rispettate adeguatamente
- Può essere migliorato attraverso l'innalzamento del livello di sicurezza e di notifica dei dispositivi informatici in dotazione

(M4.2.3.1) Insourcing

- Vuole dire svolgere un progetto, parte di esso o in generale un'attività o un servizio all'interno dell'azienda stessa, sia essa una sussidiaria o una consociata
- Può voler dire portare o riportare un'attività, normalmente svolta all'esterno, internamente all'azienda
- Si distingue nettamente dall'attività di verticalizzazione
- Può essere una strategia competitiva nel caso di progetti o attività strategiche, a forte valore aggiunto che richiedano il mantenimento (o il trasferimento) del know-how entro il perimetro aziendale
- Può essere una strategia competitiva nel caso di progetti o attività, a basso valore aggiunto ma rilevanti nelle economie di scala
- Deve considerare correttamente i costi relativi alla realizzazione dei nuovi impianti produttivi

(M4.2.3.3) Esternalizzazione l'infrastruttura IT (CED)

- Può essere necessario vista crescente complessità dei sistemi informatici
- Vuole dire una riduzione dei costi a canone
- Vuole dire eliminare i tempi morti del personale, tutto è gestito contrattualmente a corpo
- Vuole dire assistenza continua: Il contratto prevede l'assistenza continua che può arrivare a 7 giorni su 7 e 24h su 24
- Vuole dire scalabilità più semplice ma economicamente più onerosa se gestita con una infrastruttura esternalizzata
- Vuole dire Disaster Recovery gestito dal contratto

(M4.2.3.5) Esternalizzare i servizi informatici in Cloud

- Può essere una soluzione per ridurre l'onere di elaborazione in carico al CED
- Permette una riduzione dei costi fissi
- Ha sempre un aumento dei costi fissi
- Permette una maggiore accessibilità all'applicazione: È necessario, di solito, solamente un browser

- Permette una migliore scalabilità: le tariffe dei provider sono progressivamente decrescenti man mano che aumentano gli utenti
- Permette una maggior controllo dell'applicazione (es. in caso di anomalie e malfunzionamento)

(M4.2.3.7) La servitizzazione IaaS prevede

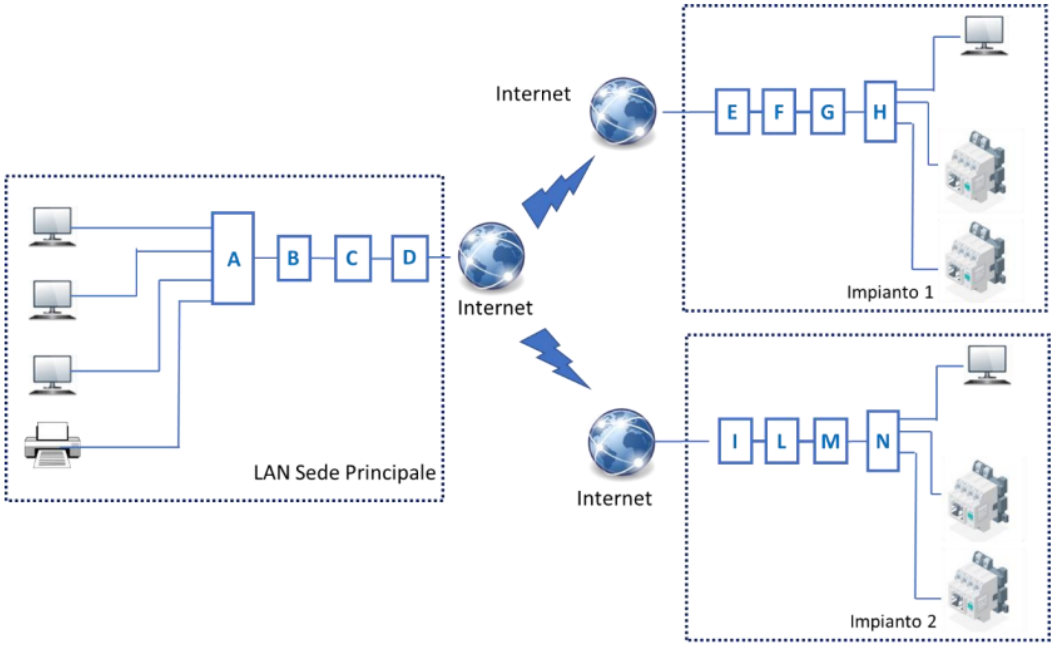
- Networking gestito dal cloud service provider
- Storage gestito dal cloud service provider
- Servers gestiti internamente
- Virtualizzazione gestita internamente
- Sistema operativo gestito internamente
- Applicazione gestita internamente

(M4.2.3.9) La servitizzazione SaaS prevede

- Networking gestito dal cloud service provider
- Storage gestito dal cloud service provider
- Servers gestiti dal cloud service provider
- Virtualizzazione gestita dal cloud service provider
- Sistema operativo gestito internamente
- Applicazione gestito internamente

Esercizio 1

Un'azienda ha realizzato la topologia di rete indicata nello schema, determinare la tipologia degli apparati di rete e dei presidi di protezione, per ciascun punto da A ad N, considerando gli standard ISO/IEC 27001 e ISA/IEC 62443



A. Switch
B. IPS (Instrusion Prevention System)
C. Firewall
D. Router
E. Router
F. Firewall
G. IPS (Intrusion Prevention System)
H. Switch
I. Router
J. (non c'è nello schema)
K. (non c'è nello schema)
L. Firewall
M. IPS (Intrusion Prevention System)
N. Switch

Esercizio 2

È necessario partizionare la rete 163.122.10.0 in 4 sottoreti così costituite:

- Sottorete A: 46 Host
- Sottorete B: 34 Host
- Sottorete C: 24 Host
- Sottorete D: 30 Host

Compilare la tabella seguente con i dati richiesti:

Sottorete	Indirizzo di sottorete	Numero Totale di Host Disponibili
A	163.122.10.0/26	62 (Utilizzati 46)
B	163.122.10.64/26	62 (Utilizzati 34)
C	163.122.10.128/27	30 (Utilizzati 24)
D	163.122.10.160/27	30 (Utilizzati 30)

Appello 8 Luglio 2022 - T1

(M1.3.1.10.1) L'incapsulamento ISO/OSI

❔ È un principio per cui in corrispondenza di ogni livello della struttura che il pacchetto dell'Host mittente attraversa, si incorporano le informazioni che sono proprie e uniche del livello attraversato

❔ È un principio per cui in corrispondenza di ogni livello della struttura che il pacchetto dell'Host mittente e destinatario attraversa, si incorporano le informazioni che sono proprie e uniche del livello attraversato

❔ È un principio per cui in corrispondenza di ogni livello della struttura che il pacchetto dell'Host Mittente attraversa si incorporano le informazioni che poi vengono eliminate man mano che si risalgono i livelli dell'Host Destinatario sino ad estrarre il messaggio originario

❔ È un principio per cui ad ogni livello ISO/OSI viene effettuato un controllo di congruenze attraverso un CRC

❔ Per funzionare necessita che ogni livello ISO/OSI offra il proprio "servizio" solamente al livello sottostante in maniera corretta

❔ Conferisce robustezza e sicurezza delle trasmissioni al modello ISO/OSI

(M1.3.2.8.1) Un cavo in fibra ottica Monomodale (PARZIALMENTE RIPETUTA)

❔ Prevede una sola modalità di propagazione: un'unica lunghezza d'onda della luce nel nucleo della fibra

❔ Ha un nucleo di vetro molto più piccolo del cavo multimodale

❔ Prevede varie modalità di propagazione, con varie lunghezze d'onda

❔ Garantisce l'assenza di interferenza o sovrapposizione tra diverse lunghezze d'onda sulle lunghe distanze

❔ Ha un nucleo di vetro da almeno 50 mm (nella tipologia OS1 e OS2)

❔ Può essere usato, indipendentemente dalla tipologia, sia al chiuso che all'aperto

(M1.3.2.11.1) L'astrazione Socket TCP è

❔ Un'istruzione software standardizzata progettata per essere utilizzabile nei programmi applicativi che permette la trasmissione e la ricezione di dati attraverso una rete

❔ La principale responsabile nello stabilire la connessione tra due host e mantenere la sessione per poi rigenerare la connessione all'invio di ulteriori pacchetti

❔ Indirettamente responsabile dello hand shake a tre livelli del TCP/IP

❔ Configurata diversamente sul client e sul server

❔ Configurata in modo che lato client e lato server abbiano identiche funzionalità

❔ Parametrizzata con due parametri Seq (Numero Sequenza) e Ack (Riconoscimento) in tre passaggi stabilisce una connessione

(M1.3.3.5.1) Il Firewall:

❔ È un dispositivo solamente hardware che funziona a livello 2

❔ Monitora il traffico in entrata e in uscita utilizzando una serie predefinita di regole di sicurezza per consentire o bloccare gli eventi

❔ Che utilizza il criterio di applicazione "Default-Deny" permette solo ciò che viene autorizzato esplicitamente, mentre il resto viene vietato

❔ Che utilizza il criterio di applicazione "Default-Deny" blocca solo ciò che viene vietato esplicitamente, mentre il resto viene permesso

❔ Utilizza normalmente per la configurazione delle regole: indirizzo IP sorgente, IP di destinazione e l'indirizzo MAC

❔ Se funziona a livello 7 può mettere in sicurezza le applicazioni Web

(M3.2.1.1.1) Lo standard ISO/IEC 27000-series

❔ È una serie di norme internazionali fuse in un unico documento che costituiscono uno standard relativo alla sicurezza delle informazioni

❔ È una serie di norme internazionali che costituiscono uno standard relativo alla sicurezza informatica

❔ È denominato "Information Security Management Systems (ISMS) Family of Standards" e si prefigge di proteggere le informazioni che vengono mantenute ed elaborate da un'organizzazione

❔ Permette alle organizzazioni di sviluppare ed implementare un proprio sistema per la gestione della sicurezza delle informazioni (SGSI)

❔ È stato generato dagli standard British Standard BS 7799-1 e -2

❔ Si focalizza sulla protezione dei dati esclusivamente attraverso il consolidamento della tecnologia di rete

(M3.2.1.5.1) ISO/IEC 27002 permette di strutturare in controlli secondo uno schema che prevede i seguenti livelli (indicare solo quelli effettivamente presenti) (RIPETUTA)

❔ Aree di controllo

❔ Aree di Rischio

- Zone Locali e Remote
- Categorie di Controllo
- Contromisure (Controlli)
- Categorie di Allarme

(M3.2.6.2.1) La struttura di ISA/IEC 62443 (RIPETUTA)

- È rappresentabile in quattro gruppi di standard che possono rappresentare: “Modelli”, “Gestione”, “Sistema” e “Componente”
- È costituita da tre famiglie di standard con vari livelli di approfondimento più uno non ancora pubblicato
- È composta dalle famiglie: “Modelli”, “Gestione”, “Organizzazione” e “Componente”
- È composta dalle famiglie: “General”, “Policy & Procedures”, “System” e “Component”
- È costituita da famiglie di standard con analogo numero di documenti in ogni famiglia

(M3.2.6.5.1) I conduits secondo ISA/IEC 62443 (RIPETUTA)

- Raggruppano gli elementi che consentono la comunicazione peer to peer tra due zone
- Forniscono funzioni di sicurezza che consentono una comunicazione sicura e permettono la coesistenza di zone con livelli differenti
- Possono essere usati per fare comunicare due o più zone fra di loro
- Consistono nel raggruppamento di cyber asset dedicati esclusivamente alle comunicazioni, e che condividono gli stessi requisiti di cybersecurity
- Possono attraversare più di una zona in siti con differenti locazioni geografiche
- Possono avere sotto-conduits per una difesa in profondità

(M3.3.5.1.1) La Direttiva NIS (Network and Information Security) (RIPETUTA PARZIALE)

- È il primo atto legislativo sulla sicurezza informatica approvato dall’Unione Europea
- È entrata in vigore in Italia 24 giugno 2018 mediante il D.L. n. 65 del 24 18 maggio 2018
- Impone la notifica obbligatoria degli incidenti all'Autorità nazionale istituita allo scopo
- Impone la nascita di CSIRT (Computer Security Incident Response Team) nazionali, sulla base del CERT-UE
- Stabilisce l’obiettivo dell’adozione di una serie di misure di sicurezza comuni che potranno essere adottate discrezionalmente dai singoli paesi
- Impone di realizzare un network nei singoli paesi che si occupi della sicurezza delle reti critiche

(M3.4.5.2) Un sistema di Anomaly Detection (PARZIALMENTE RIPETUTO)

- Permette di trovare e correggere gli incidenti non appena iniziano a verificarsi e prima che possano causare danno per l’organizzazione
- Permette di trovare e correggere gli incidenti dopo che si sono verificati in modo da minimizzare i danni all’organizzazione

? Utilizza un approccio di Machine Learning per monitorare l'insieme dei dati, apprendere il comportamento di ogni dispositivo e fornire avvisi puntuali sugli errori critici

? Utilizza un approccio con logiche algoritmiche tradizionali basate su modelli predefiniti

? Realizza il "deep packed inspection"

? Definisce la "Baseline" ovvero la "conoscenza o linea di base" di quella specifica architettura di rete

(M3.4.5.4) L'Endpoint protection

? Realizza il tunneling nella comunicazione dall'interno all'esterno dell'azienda

? Si riferisce alla protezione di qualsiasi dispositivo o connessione che abbia accesso alla rete aziendale

? Può utilizzare tecniche di Machine learning per rilevare le minacce zero-day

? Non ha mai un firewall integrato

? Può realizzare la Mobile security (cellulari, tablet e laptop)

(M4.1.1.1) Quali tra le seguenti caratteristiche rientrano nel modello di Burocrazia secondo Max Weber (RIPETUTA PARZIALMENTE)

? Fedeltà al marchio

? Competenza disciplinata

? Diritto di licenziare

? Gerarchia degli uffici

? Preparazione specializzata

? Concorsi pubblici per l'assunzione

(M4.1.1.3) Chi tra questi personaggi ha posto le basi degli attuali modelli organizzativi

? Karl Marx

? Alessandro Volta

? Karl Emil Maximilian Weber

? Enrico Fermi

? Thomas Robert Malthus

? Adam Smith

(M4.1.1.5) Quali di questi sono principi fondamentali di organizzazione aziendale (indicare vero)

? Dividere l'azienda per raggruppamenti funzionali omogenei (dipartimenti, divisioni, ecc.)

? Dividere l'azienda per raggruppamenti verticali o orizzontali

? Definire ruoli e mansioni nei singoli raggruppamenti

? Accentrare la responsabilità in poche figure che evitano massimamente la delega

? Modellizzare i processi aziendali in una prospettiva di miglioramento continuo

- Standardizzare i processi

(M4.1.1.7) Quali di questi sono principi fondamentali di organizzazione aziendale (indicare vero)

- Pianificazione aziendale e Pianificazione strategica
- Gestire gli obiettivi, le priorità e i carichi di lavoro correttamente
- Ogni persona che fa parte dell'organizzazione deve aver chiaro in mente il proprio compito
- Ogni dipendente deve agire sempre e solo con il coordinamento del supervisore
- Ogni persona deve avere responsabilità e obiettivi ben definiti
- Ogni risorsa umana deve aver chiaro i limiti del proprio ruolo

(M4.1.1.9) Cosa significa Costruire una Struttura Organizzativa?

- Scegliere l'assetto legale che si ritiene più appropriato rispetto al numero e le capacità dei dipendenti (impresa individuale o impresa di capitali o altro)
- Scegliere l'assetto legale che si ritiene più appropriato rispetto allo scopo aziendale (impresa individuale o impresa di capitali o altro)
- Dare «ordine» alle parti e ai loro compiti; creando un assetto organizzativo stabile, ancorché modificabile
- Definire «regole» e «procedure» di comportamento delle parti e dei partecipanti
- Definire «regole» e «procedure» di comportamento dei fornitori e dei "competitors"
- Progettare il modello, ovvero la configurazione, dell'assetto organizzativo che è rappresentato dall'organigramma dell'impresa

(M4.1.1.11) L'Organigramma (RIPETUTA)

- Rappresenta i dipendenti e le posizioni attraverso caselle o altre forme su vari livelli, linee dritte o a gomito collegano insieme tali livelli
- Riproduce parzialmente la struttura interna di un'organizzazione o un'azienda
- È una rappresentazione visiva della gerarchia e dei ranghi delle persone, delle aree funzionali o dei raggruppamenti che compongono l'organizzazione
- Può rappresentare strutture organizzative Iper-dimensionali
- Può rappresentare strutture organizzative per Area Geografica
- Può rappresentare strutture organizzative Divisionali

(M4.1.1.13) La Struttura Organizzativa Divisionale

- È la soluzione organizzativa dove tutte le attività (produzione, marketing, finanza, ecc.) vengono raggruppate in una unica divisione aziendale
- È la soluzione organizzativa dove tutte le attività (produzione, marketing, finanza, ecc.) inerenti a un prodotto o servizio vengono raggruppate in una divisione
- È la soluzione organizzativa dove ogni divisione corrisponde ad una unità organizzativa
- Facilita la realizzazione della strategia di diversificazione produttiva

? Permette la concentrazione delle attività relative ad uno specifico prodotto o servizio permettendo una maggiore flessibilità delle operazioni

? Permette un migliore coordinamento delle attività della divisione ma rende più complessa la misurazione delle performance di ciascuna divisione rispetto alle altre

(M4.1.1.15) La Struttura Organizzativa Divisionale per Area Geografica

? Prevede che ogni divisione corrisponda ad una unità organizzativa che fa parte di un gruppo

? Prevede che ogni divisione sia strettamente e rigidamente legata alla direzione generale centrale

? Facilita la comunicazione tra le unità operative dell'area

? Riduce i costi di trasporto, permettendo maggiore efficienza nella distribuzione

? Permette di adattare il prodotto alle specificità locali e interpretare rapidamente i cambiamenti nei gusti dei consumator

? Non ha sostanziali svantaggi o rischi essendo gli uffici di direzione (centrale di area) decentralizzati

(M4.1.2.1) Il modello Weil Broadbent per l'allineamento tra reparto IT e il Business:

? Illustra come il Piano Strategico Aziendale può influenzare la Strategia ICT che ne rimane completamente indipendente

? Illustra come il Piano Strategico Aziendale guidi la Strategia ICT per un vantaggio competitivo

? Delinea come la Strategia ICT allinei il Portfolio IT

? Delinea come il Portfolio IT allinei la Strategia ICT

? Delinea come i vincoli (normativi, concorrenza, tecnologia, ecc.) influenzino il Piano Strategico e il Portfolio IT

? Delinea come il Portfolio IT abiliti e informi il piano strategico aziendale

(M4.1.3.2) Indicare con vero quali dei seguenti sono compiti del CIO (Chief Information Officer) (RIPETUTA PARZIALMENTE)

? Contribuire all'analisi e alla definizione dei processi aziendali, raccogliendo e razionalizzando le esigenze dei vari comparti

? Definire, insieme alla direzione, gli obiettivi aziendali ed il contributo dell'informatica per il loro raggiungimento

? Definire il Safety Plan (SP) per l'azienda

? Definire e gestire il budget destinato ai Sistemi Informativi e coordinare il reparto IT

? Avere competenze sulla tecnologia anche se non approfondite

? Partecipare alla definizione dei requisiti funzionali e architetturali degli strumenti informativi da introdurre in azienda

(M4.1.3.4) Indicare con vero quali dei seguenti sono compiti del CISO (Chief Information Security Officer)

? Realizzare assessment della sicurezza: per valutare lo stato dell'arte della sicurezza in azienda e individuare un piano strategico per aumentare la capacità di reagire alle cyber minacce

? La definizione delle policy di sicurezza: definire regole e standard per la gestione della sicurezza

? La definizione delle policy e degli standard informatici: per le architetture tecnologiche di rete e di sistema

? L'analisi del rischio cyber: comprendere le vulnerabilità e le minacce per l'azienda per compiere scelte adeguate alla gestione del rischio cyber in termini di politiche e strumenti

? La definizione delle architetture di sicurezza: disegnare l'architettura per la gestione della sicurezza e monitoraggio delle scelte strutturali

? Condurre ricerche ed eseguire soluzioni di gestione della Sicurezza (Safety) per aiutare a mantenere al sicuro le persone

(M4.1.3.6) Il DPO (Data Protection Officer) secondo il GDPR

? È responsabile del monitoraggio della conformità dell'organizzazione per la quale lavora e svolge il ruolo di punto di contatto tra gli interessati e l'autorità di controllo competente

? Informa e consiglia l'organizzazione ed i suoi dipendenti circa gli obblighi di protezione dei dati ai sensi del GDPR

? Monitora la conformità dell'organizzazione al Regolamento ed alle policy e procedure interne in materia di protezione dei dati

? Deve essere obbligatoriamente nominato, sia per le aziende pubbliche che per quelle private

? Funge da punto di contatto per l'autorità di controllo per tutte le questioni inerenti alla protezione dei dati, come la segnalazione di violazioni dei dati

? Deve essere obbligatoriamente un dipendente dell'organizzazione

(M4.1.5.2) Il Security Analyst

? Previene, rileva e gestisce le minacce informatiche, nell'ottica di proteggere computer, dati, reti e programmi delle aziende

? Conosce le tecniche crittografiche

? Conosce i protocolli di comunicazione

? Conosce i sistemi di autenticazione e controllo

? Non si occupa degli aspetti giuridici e delle normative internazionali (in carico al DPO)

? Si appoggia a consulenti esterni per quel che riguarda l'Intrusion Detection

(M4.1.5.4) L'Informatico Forense

? È un tecnico coinvolto nella raccolta di dati circa l'utilizzo di sistemi, reti e applicazioni e analisi degli stessi in relazione ad incidenti di cybersecurity

? Si appoggia sempre alla polizia per le indagini

- Si occupa anche di redigere una documentazione idonea alla presentazione in sede processuale
- È conosciuto formalmente anche come “Analista forense”
- È conosciuto formalmente anche come “Analista processuale”
- Ha competenze IT e degli strumenti software per le indagini forensi

(M4.2.2.2) Quali di questi elementi fanno parte di un buon piano operativo per diffondere la sicurezza informatica (indicare con vero)

- Definire gli obiettivi di sicurezza
- Realizzare attacchi di Phishing simulati
- Predisporre corsi di formazione e test di valutazione
- Pianificare accuratamente attività a lungo termine
- Coinvolgere solo chi è coinvolto direttamente con incarichi ciritici
- Prepararsi adeguatamente in caso di errori umani

(M4.2.3.2) Outsourcing

- È una strategia aziendale in base alla quale un progetto, parte di esso o in generale un’attività o un servizio viene trasferita a un'azienda esterna
- Si realizza per concentrarsi meglio sugli aspetti centrali del business
- Si realizza per concentrarsi meglio sugli aspetti centrali della cyber security
- Può migliorare l'efficienza e la produttività
- Può provocare perdita di controllo su conoscenze specifiche (know How) e generare rischi di tipo organizzativo
- Può generare rischi di tipo organizzativo ma non la perdita di controllo su conoscenze specifiche (know How)

(M4.2.3.4) Esternalizzare l’infrastruttura IT (CED)

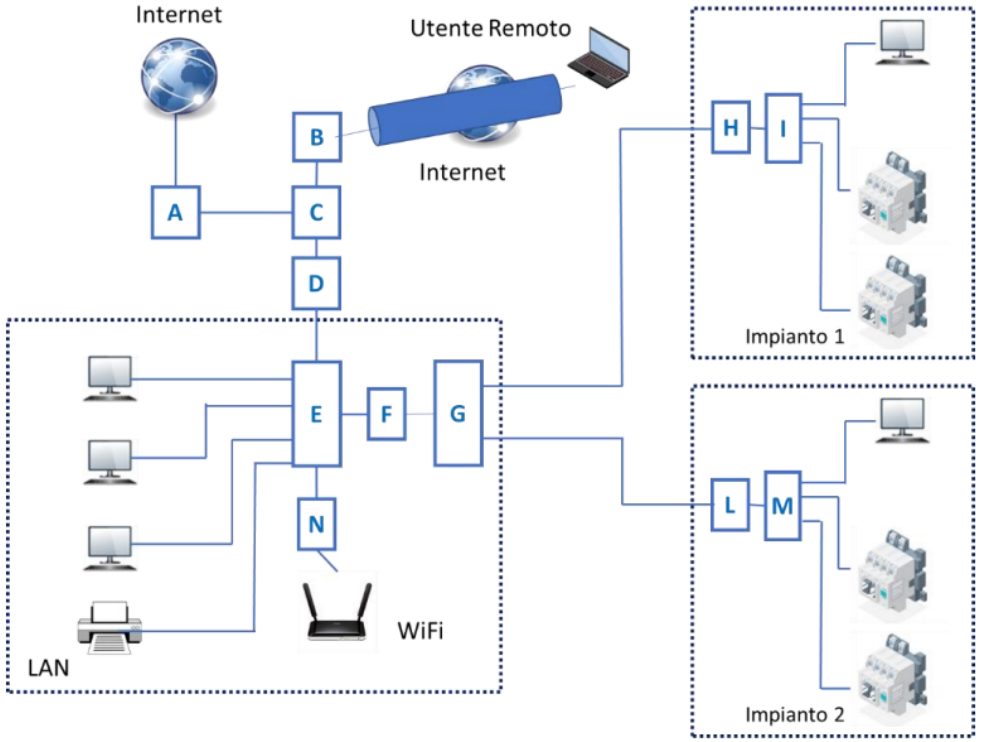
- Può essere necessario per contenere i costi dell’infrastruttura informatica al crescere dell’azienda
- Il costo del servizio può diventare molto oneroso se non sono dimensionati correttamente i requisiti (funzioni, latenza e disponibilità)
- Non porta mai a sorprese in relazione al livello, la qualità e la modalità di erogazione del servizio
- Può essere problematico se non è correttamente definito il contratto, quello che non è chiaramente scritto non si ritrova quando è necessario
- È sempre sinonimo di messa in sicurezza del dato anche in relazione alla sua proprietà, mai nessun leak
- Può portare a difficoltà di coordinazione tra le attività interne ed esternalizzate

(M4.2.3.8) La servitizzazione PaaS prevede

- ? Networking gestito dal cloud service provider
- ? Storage gestito dal cloud service provider
- ? Server gestito dal cloud service provider
- ? Virtualizzazione gestita internamente
- ? Sistema operativo gestito internamente
- ? Applicazione gestita internamente

Esercizio 1

Un'azienda ha realizzato la topologia di rete indicata nello schema, determinare la tipologia degli apparati di rete e dei presidi di protezione, per ciascun punto da A ad N, considerando gli standard ISO/IEC 27001 e ISA/IEC 62443.



A. Router
B. VPN
C. Firewall
D. IPS (Intrusion Prevention System)
E. Switch
F. Firewall
G. Switch
H. Firewall
I. Switch
J. Firewall
K. Switch
L. Switch

Esercizio 2

È necessario partizionare la rete 185.152.20.0 in 4 sottoreti così costituite:

- Sottorete A: 30 Host
- Sottorete B: 58 Host
- Sottorete C: 20 Host
- Sottorete D: 22 Host

Compilare la tabella seguente con i dati richiesti:

Sottorete	Indirizzo di sottorete	Numero Totale Host Disponibili
A	185.152.20.0/27	30 (Utilizzati 30)
B	185.152.20.32/26	62 (Utilizzati 58)
C	185.152.20.96/27	30 (Utilizzati 20)
D	185.152.20.128/27	30 (Utilizzati 22)

Appello 23 Settembre 2022 T1

(M1.1.2.9) La banda di trasmissione SHF

- ❔ Identifica una banda di frequenze dove si trovano anche le microonde
- ❔ Identifica una banda di frequenza super-lunghe
- ❔ Identifica una banda di frequenze super-alte
- ❔ Ha una banda di frequenze che va da 30 a 300MHz
- ❔ Ha una banda di frequenze che va da 3 a 30 Ghz
- ❔ È utilizzata dai Radar, dai link a microonde e dalle comunicazioni satellitari

M1.1.3.2) Il Routing

. ❔ Il Routing è l'instradamento effettuato tra reti differenti con l'ausilio delle tabelle di instradamento configurate a livello dei router

❔ Il Routing è l'instradamento effettuato all'interno della stessa rete con l'ausilio delle tabelle di instradamento configurate a livello dei router

❔ Per il suo funzionamento considera che i router siano a conoscenza degli indirizzi solo delle reti a cui sono direttamente collegati

❔ Per il suo funzionamento considera che i router siano a conoscenza degli indirizzi delle reti a cui sono direttamente o indirettamente collegati

❔ Nella tabella di instradamento ogni riga corrisponde a una regola e le regole vengono esaminate dalla prima all'ultima, se ci sono più regole che corrispondono all'indirizzo fornito, viene scelta la regola che ha più bit in comune con l'indirizzo fornito

❔ Nella tabella di instradamento ogni riga corrisponde a una regola e le regole vengono esaminate dalla prima all'ultima, se ci sono più regole che corrispondono all'indirizzo fornito, viene scelta la prima regola che viene esaminata

(M1.1.3.5) Un indirizzo IPv4

- ❔ Ha la dimensione di 32 bits, divisi in 4 gruppi da 8 bits ☕
- ❔ Ha la dimensione di 32 bits, divisi in 8 gruppi da 4 bits
- ❔ Ha la dimensione di 128 bits, divisi in 8 gruppi da 16 bits
- ❔ Ha la dimensione di 256 bits, divisi in 8 gruppi da 32 bits

- Può essere assegnato solo dall' InterNIC (InterNetwork Information Center)
- Può essere assegnato da chiunque

(M1.1.4.2) L'Uniform Resource Locator (URL)

- È una sequenza di caratteri che identifica univocamente l'indirizzo di una risorsa presente su un host (server) che fa parte di una rete di computer e resa accessibile a un client
- È una sequenza di caratteri esclusivamente alfanumerici
- Identifica univocamente gli indirizzi delle risorse come documenti, un'immagini, video, tipicamente presente sui server
- Può utilizzare protocolli http, https, ftp o mms
- Si avvale del DNS (Domain Name System) per "risolvere" l'URL in indirizzo IP
- Nel caso utilizzi il protocollo https realizza una comunicazione client server non criptata

(M1.1.6.1) Una Minaccia alla sicurezza informatica

- Può essere definita come un codice eseguibile che, utilizzando un vettore esterno o interno al perimetro aziendale, ha la capacità di compiere operazioni dannose per la macchina in cui si trova, per il sistema informatico in cui si è inserito o per i dati in esso contenuti o gestiti
- Si propaga e si concretizza sempre indipendentemente dal fattore umano
- Utilizza un vettore che può essere un attacco diretto o indiretto da parte di qualche malintenzionato o un incidente anche accidentale
- Può essere eliminata mediante l'installazione di un buon antivirus
- Può penetrare qualsiasi tipo di file eseguibile e diffondersi nel momento in cui il file viene copiato e inviato da un utente all'altro
- Può essere costituita dai Ransomware

(M1.3.1.15) Quali delle seguenti funzioni appartengono al livello ISO/OSI di Collegamento (2)

- Identificare i nodi connessi
- Controllare gli errori
- Correggere gli errori mediante trasmissione
- Indirizzamento logico
- Incapsulamento del Pacchetto
- Gestione delle Connessioni

(M1.3.4.2) La rete MAN (Metropolitan Area Network)

- È una rete di telecomunicazione a banda stretta, che collega più LAN geograficamente vicine
- È di solito utilizzata da singole filiali di un'azienda che vengono connesse ad una MAN attraverso l'affitto di linee dedicate
- Utilizza connessioni in fibra ottica, che consentono prestazioni migliori

- Ha una velocità di trasferimento tra due nodi distanti molto più lenta della comunicazione interna di una LAN
- Ha un'infrastruttura che viene messa a disposizione da provider che operano a livello internazionale
- A livello cittadino si collega a reti sovraregionali e internazionali, chiamate Wide Area Network (WAN)

(M2.2.1.3) Quali strategie posso utilizzare per mitigare i possibili danni da un attacco cyber ad una linea produttiva (al momento l'unica che produce un determinato bene)?

- Ridondare e rendere indipendenti le architetture di rete e i dispositivi informatici che gestiscono le macchine di produzione
- Realizzare un adeguato sistema di segmentazione e segregazione delle reti e degli apparati di controllo
- Aumentare gli stock delle materie prime
- Valutare, compatibilmente con i costi, la realizzazione di una linea produttiva parallela analoga
- Aumentare considerevolmente la quantità di prodotti finiti in magazzino
- Isolare completamente la rete industriale dalla rete office

(M2.2.2.2) Un incidente informatico interno all'organizzazione

- Può essere qualsiasi evento che sottintende una violazione delle politiche di sicurezza IT fonte di danno per gli asset IT
- Può essere un incidente collegato ad un attacco con obiettivi economici e può avere come obiettivi i sistemi Amministrativi e gestionali o i sistemi di progettazione
- In ogni caso è di rilevanza inferiore rispetto ad un attacco diretto
- Può essere un incidente collegato ad un attacco avente come obiettivo l'interruzione del servizio e come obiettivi i sistemi amministrativi e gestionali, i portali web e di e-commerce i sistemi di produzione
- Di solito è molto semplice verificare il nesso causa-effetto tra evento rilevato e danno subito
- Può essere un incidente informativo casuale legato ad un'operazione o una procedura errata

(M2.3.1.4) Nella Gestione Aziendale le Operazioni Soggettive possono essere:

- Reperimento di mezzi finanziari
- Attività decisionali
- Investimenti
- Attività di controllo
- Disinvestimento

(M2.3.1.5) L'ERP aziendale

- È l'Enterprise Resource Planning
- È Il Sistema Gestionale Aziendale
- Non fa parte del sistema informativo aziendale

- È un software
- È un hardware
- Può essere un servizio in cloud

(M2.3.2.3) L'Organigramma (RIPETUTA)

- È la rappresentazione grafica della struttura di una organizzazione
- Rappresenta i legami funzionali e gerarchici che tengono unite le persone all'interno dell'organizzazione stessa
- Rappresenta solamente i legami funzionali che tengono unite le persone all'interno dell'organizzazione stessa
- Può essere di tipo Funzionale
- Può essere di tipo Perimetrale
- Può essere Matriciale

(M2.3.2.4) In ogni Organizzazione

- La Mansione deve essere assegnata a ogni individuo
- Può non essere associata una Mansione specifica ad un individuo
- Il Ruolo è l'insieme dei comportamenti previsti da una specifica figura professionale
- La Posizione è lo stato o il grado assegnato ad una figura professionale
- Ad ogni risorsa vanno assegnate delle responsabilità per raggiungere degli obiettivi aziendali comuni
- Le stesse mansioni i ruoli e le posizioni aziendali possono essere attribuite a più persone contemporaneamente

(M3.1.1.5) Quali dei seguenti sono i principali processi di Cyber Security (indicare Vero)

- Monitoraggio degli Incidenti Informatici
- Gestione delle performance di rete
- Gestione degli incidenti informatici
- Gestione delle vulnerabilità
- Gestione delle obsolescenze
- Gestione delle risorse

(M3.1.1.6) Il SOC

- È il Security Operations Center
- È il Security Organization Center
- È un centro da cui vengono forniti servizi finalizzati alla sicurezza dei sistemi informativi dell'azienda stessa
- Può essere solo interno all'organizzazione

? Può anche fornire servizi di Incident Response, in questo caso svolge la funzione di CERT (Computer Emergency Response Team)

? Può avere anche funzioni di CSIRT (Computer Security Incident Response Team)

(M3.1.2.2) Perché bisogna modellare (modellizzare) i processi aziendali?

? Per fornire una descrizione di una sequenza di attività comprensibile ad un osservatore esterno al processo

? Perché la legislazione lo richiede obbligatoriamente

? Per usare un modello grafico standardizzato con l'obiettivo di presentare un documento in un formato facilmente comprensibile ad organizzazioni differenti

? Per descrivere cosa attualmente succede durante un processo

? Per descrivere anche cosa si desidererebbe far succedere durante un processo in futuro

? Per creare la base e i presupposti all'analisi per l'innovazione di processo

(M3.1.2.3) Quali sono le tipologie di Modellizzazione?

? Basata sui dati

? Basata su attività

? Basata su informazioni

? Basata su transazioni

? Basata su messaggi

? Basata su comunicazione

(M3.1.3.4) Perché le SOP (Standard Operating Procedure) sono importanti?

? Aiutano l'organizzazione a soddisfare gli standard di conformità

? Supportano ma non garantiscono che le attività aziendali non abbiano impatti ambientali negativi

? Semplificano e massimizzano la produzione/output

? Stabiliscono degli standard di sicurezza (fisica e logica)

? Supportano la formazione e la crescita professionale del personale

? Garantiscono sempre risultati coerenti

(M3.2.1.11) Quali dei seguenti gruppi di norme fanno parte della famiglia degli Standard ISO/IEC 27000?

? Norme che descrivono una panoramica e la terminologia o vocabolario

? Norme che specificano i requisiti

? Norme che identificano i processi

? Norme che descrivono le linee guida dettagliate

? Norme che descrivono le linee guida negli specifici ambiti/settori

? Norme aggiunte che descrivono delle direttive specializzate

(M3.2.5.1) Quali delle seguenti sono effettive differenze tra NIST Cyber Security Framework e ISO 27001

? Il NIST è stato creato principalmente per la gestione del rischio sulle informazioni, ISO 27001 è invece un approccio riconosciuto a livello internazionale per la creazione e il mantenimento di un ISMS

? ISO 27001 è volontario, mentre il NIST CSF prevede la certificazione

? I framework NIST hanno vari cataloghi di controllo e cinque funzioni per personalizzare i controlli di sicurezza informatica, mentre l'allegato A ISO 27001 (2013) fornisce 14 categorie di controllo con 114 controlli e 7 clausole di gestione per guidare le organizzazioni attraverso i loro ISMS

? La ISO 27001 è meno tecnica, con maggiore enfasi sulla gestione basata sul rischio

? La ISO 27001 è più tecnica, con minore enfasi sulla gestione basata sul rischio

? La ISO 27001 è una buona scelta per certificare le organizzazioni che hanno maturità operativa, mentre il NIST CSF può essere più adatto per le organizzazioni che si trovano nelle fasi iniziali dello sviluppo di un programma di rischio per la sicurezza informatica

(M3.3.1.2) Quali sono le origini legislative del diritto alla privacy italiano?

? Costituzione Italiana, articoli 14, 15 e 21, riguardanti il domicilio, la libertà e segretezza della corrispondenza, e la libertà di manifestazione del pensiero

? Costituzione Italiana articolo 2, come anche sostenuto la Corte Costituzionale con la sentenza n. 38 del 1973

? Sentenza della Corte di Cassazione n. 4487 del 1961

? Sentenza della Corte di Cassazione n. 4487 del 1956

? Prima legge italiana di tutela della privacy, Legge 675 del 1996, come attuazione della direttiva 95/46/CE

? Prima legge italiana di tutela della privacy, Legge 675 del 1998, come attuazione della direttiva 95/46/CE

(M3.3.1.3) Quali sono le attuali leggi italiane sulla privacy?

? <

? Il Regolamento UE 2016/697 del Parlamento Europeo e del Consiglio del 27 aprile 2016, cosiddetto GDPR (General Data Protection Regulation) attraverso il D. L. di adeguamento 10 agosto 2018, n. 101, dal D.M. n. 15 marzo 2019 e dal D.L. 14 giugno 2019, n. 53

? Il Regolamento UE 2016/679 del Parlamento Europeo e del Consiglio del 25 aprile 2016, cosiddetto GDPR (General Data Protection Regulation) attraverso il D.L. di adeguamento 10 agosto 2018, n. 101, dal D.M. n. 15 marzo 2019 e dal D.L. 14 giugno 2019, n. 53

? Il Regolamento UE 2016/679 del Parlamento Europeo e del Consiglio del 27 aprile 2016, cosiddetto GDPR (General Data Protection Regulation) attraverso il D.L. di adeguamento 10 agosto 2018, n. 101, dal D.M. n. 15 marzo 2019 e dal D.L. 14 giugno 2019, n. 53

(M3.3.2.3) Il Patent Infringement

? È inteso come la violazione dei diritti di proprietà intellettuale o di brevetto

? Per la legge italiana è assimilato al reato di furto

? Per la legge italiana è assimilato al reato di contraffazione

? È in costante aumento grazie al grande sviluppo dell'e-commerce e l'utilizzo dei social media per finalità di marketing

? Riguarda beni di lusso e griffati, alimentari, farmaci (con tutte le implicazioni relative alla salute pubblica), ecc.

? Anche se non arreca un enorme danno economico sia ai titolari dei diritti che ai consumatori è comunque un fenomeno sotto osservazione

(M3.3.5.4) Quali dei seguenti sono effettivamente Operatori di Servizi Essenziali (OES) secondo NIS

? Impresa elettrica

? Distributore locale di carburante per autotrazione

? Gestori del sistema di distribuzione energia elettrica

? Gestori di sistema di trasmissione energia elettrica

? Gestori del sistema di distribuzione gas

? Gestori del sistema di tele-trasmissione gas

(M3.3.5.5) Quali delle seguenti sono funzioni del CSIRT (Computer Security Incident Response Team) nazionale?

? Il monitoraggio degli incidenti a livello nazionale ed internazionale

? L'emissione di preallarmi, allerte, annunci e divulgazione di informazioni alle parti interessate in merito a rischi e incidenti

? La delega dell'attività di intervento in caso di incidente

? L'analisi dinamica dei rischi e degli incidenti

? La sensibilizzazione situazionale

? La partecipazione alla rete europea dei CSIRT

(M3.3.5.6) Chi sono i DSP (Digital Service Providers) secondo la Direttiva NIS?

? Cloud Computing Services

? Cloud Virtual Machines

? Online Market Places

? Online Search Engines

? Online products e-commerce

. ? Online people recruitments

(M3.3.6.6) Il principio di "Accountability" del GDPR

? È un concetto che può essere tradotto in italiano come responsabilizzazione/rendicontazione

? È un concetto che può essere tradotto in italiano come contabilità

? Dispone che il titolare del trattamento adotti politiche e attui misure adeguate a garantire che il trattamento dei dati personali sia conforme allo stesso Regolamento

❔ Prevede l’adozione di comportamenti proattivi e tali da dimostrare la concreta adozione di misure finalizzate ad assicurare la corretta applicazione del regolamento

❔ Prevede l’adozione di criteri di "data protection by default and by design" ovvero che la protezione dei dati deve essere da progetto e indipendente dall’eventuale autorizzazione al trattamento

❔ Dispone che il titolare del trattamento adotti politiche e attui misure adeguate a garantire ed essere in grado di dimostrare che il trattamento dei dati personali effettuato sia conforme allo stesso Regolamento

(M3.4.1.1) Quali dei seguenti requisiti ISO 27001 possono rappresentare la fase PLAN del ciclo PDCA

❔ Contesto

❔ Leadership

❔ Pianificazione

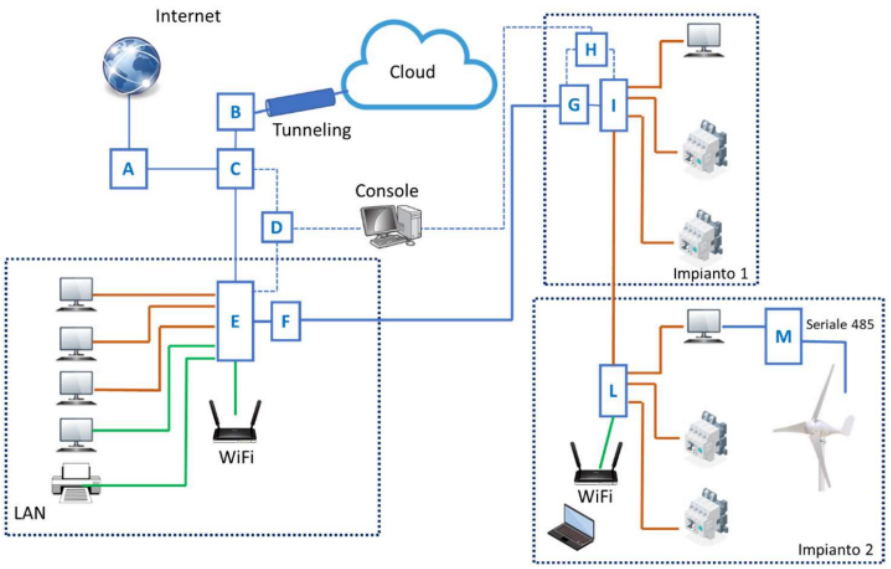
❔ Supporto

❔ Attività Operative

❔ Valutazione delle Prestazioni

Esercizio 1

Data la seguente topologie di rete:



Indicare la tipologia degli apparati e sistemi nei quadrati e rettangoli

A. Router
B. VPN
C. Firewall
D. Anomaly Detection System
E. Switch
F. FIrewall
G. Firewall
H. Anomaly Detection System
I. Switch
J. Switch
K. Gateway

Indicare la tecnologia che permette di configurare i segmenti di rete marroni e verdi VLAN

Esercizio 2 ❗

Partizionare la rete 192.168.10.0 in 4 sottoreti così costituite, ogni sottorete deve essere suddivisa in due VLAN uguali. Rappresentare le sottoreti con la notazione /X ed esplicitare il numero totale degli Host della sottorete:

- Sottorete A: 126 Host
- Sottorete B: 30 Host
- Sottorete C: 12 Host
- Sottorete D: 62 Host

					VLAN	N° Totale Host Utilizzabili
192	168	10	0	/25	1	63
192	168	10	0	/25	2	63
192	168	10	128	/27	3	15
192	168	10	128	/27	4	15
192	168	10	160	/28	5	7
192	168	10	160	/28	6	7
192	168	10	176	/26	7	31
192	168	10	176	/26	8	31

Appello 23 settembre 2022 - T2

(M3.4.2.1) Il posizionamento dello standard ISA/IEC 62443 nello stack ISA 95 (Purdue Model)

- ? Prevede i seguenti elementi in ordine di importanza: Affidabilità-> Sicurezza Fisica->Impatto sul Prodotto o sul Servizio
- ? Prevede i seguenti elementi in ordine di importanza: Affidabilità ->Impatto sul Prodotto o sul Servizio->Sicurezza Fisica
- ? Prevede i seguenti elementi in ordine di importanza: Sicurezza Fisica->Affidabilità->Impatto sul Prodotto o sul Servizio
- ? Prevede un diverso ordine di importanza per i fattori CIA: Disponibilità (Accessibilità)-> Integrità-> Riservatezza
- ? Prevede un diverso ordine di importanza per i fattori CIA: Integrità-> Riservatezza-> Disponibilità (Accessibilità)
- ? Prevede un diverso ordine di importanza per i fattori CIA: Riservatezza-> Disponibilità (Accessibilità)-> Integrità

(M4.1.2.2) Quali sono le ragioni per cui il reparto di Information Technology può essere considerato come un centro di costo?

- ? Scarsa sensibilità e skill digitali del top management
- ? Scarse risorse da dedicare ai progetti digitali
- ? Scarsa capacità di ideare e portare a termine i progetti
- ? Scarso o nessun impatto della digitalizzazione sul business dell'azienda
- ? Scarsa propensione allo sviluppo commerciale globale, azienda fortemente locale
- ? Scarsa competitività dell'azienda (possibile azienda in regime di monopolio)

(M4.2.1.1) Quali sono i maggiori rischi cyber per le Organizzazioni Bancarie e Finanziarie?

- ? Finanziario e di mancanza di erogazione del servizio al pubblico
- ? Finanziario e di continuità del business
- ? Finanziario e di diffusione di dati sensibili
- ? Fisico e di continuità di erogazione del servizio al pubblico
- ? Reputazionale e di continuità del business
- ? Terroristico e di possibile bersaglio strategico

(M1.3.1.21) Quali funzioni prevede il livello ISO/OSI Applicazione (7)

- ? Scambio di e-mail
- ? Compressione dei dati
- ? Accesso ai database
- ? Accesso ai siti Web

- Gestione remote di applicazioni distribuite
- Formattazione

(M1.3.1.22) Quali di questi livelli ISO/OSI sono livelli logici legati ai mezzi di trasmissione

- Livello 1 - Fisico
- Livello 2 - Collegamento
- Livello 3 - Rete
- Livello 4 - Trasporto
- Livello 5 - Sessione
- Livello 6 - Presentazione

(M1.3.1.23) La comunicazione tra gli omologhi livelli dello stack ISO/OSI

- È Sempre una comunicazione logica
- È sempre una comunicazione fisica
- È una comunicazione logica per i livelli dal 2 al 7 e fisica per il livello 1
- È una comunicazione logica per i livelli dal 1 al 6 e fisica per il livello 7
- È una comunicazione logica per i livelli dal 1 al 3 e fisica per i livelli dal 4 al 7
- È sempre tra un Host mittente e un Host destinatario

(M4.1.1.17) La Pianificazione Operativa

- La pianificazione operativa è il processo attraverso il quale l'impresa definisce gli obiettivi da raggiungere e le azioni per raggiungere tali scopi nel breve periodo
- Può essere rappresentata dagli obiettivi strategici che si intendono raggiungere nel medio periodo
- Può essere rappresentata dagli obiettivi che si vogliono raggiungere nell'anno di attività dell'azienda
- È sempre rappresentata dalla mission dell'azienda a lungo termine
- Si distingue da Pianificazione Tattica e Strategica che definiscono gli obiettivi, rispettivamente di medio e lungo periodo
- Può essere denominata anche Pianificazione Sinergica o Evolutiva

(M2.1.2.8) Le Società di Persone

- Per legge non hanno un importo minimo per il capitale sociale
- Per legge hanno un importo minimo per il capitale sociale
- Non prevedono organi sociali, ogni socio illimitatamente responsabile può amministrare
- Possono prevedere più organi sociali ognuno con le proprie competenze
- Hanno un'autonomia patrimoniale definita "perfetta": i soci sono personalmente responsabili delle obbligazioni sociali, solo i beni conferiti sono formalmente di proprietà della società

- Hanno un'autonomia patrimoniale definita "imperfetta": i creditori sociali possono agire sul patrimonio personale dei singoli soci ma solo dopo aver escusso infruttuosamente sul patrimonio sociale

(M2.1.2.9) Le Società S.p.A.

- Sono società di persone
- Sono società di Capitali
- Sono Società a responsabilità illimitata dell'imprenditore
- Sono società a responsabilità limitata dell'imprenditore
- Sono Società a responsabilità dei soci limitata al capitale sottoscritto
- Sono Società a responsabilità dei soci illimitata oltre al capitale sottoscritto

(M2.1.3.5) Un'azienda che distribuisce gas ed elettricità

- Appartiene al settore delle Utility
- Può essere definita anche Multiutility
- Può essere un'infrastruttura critica
- Può essere un Operatore di Servizi Essenziali
- È un'azienda manifatturiera
- Appartiene al settore secondario

(M2.2.1.4) A che tipi di rischio si può incorrere in caso di attacco Cyber al sistema gestionale aziendale?

- Rischio generale per la salute umana
- Rischio di emissioni nocive per l'ambiente
- Rischio violazione dati sensibili e Privacy
- Rischio Business Continuity
- Rischio Service Continuity
- Rischio economico

(M2.2.2.3) Il Vettore di Attacco può sfruttare tipicamente

- Vulnerabilità informatiche e mancato aggiornamento del software
- Gestione di identità e permessi non adeguata
- Meccanismi di autenticazione deboli
- App malevole
- Obsolescenza
- Mancanza di conoscenza da parte del personale

(M3.1.1.7) Quali sono le fasi del processo di monitoraggio e gestione degli incidenti informatici?

? Una fase di Preparazione Iniziale e poi un ciclo composto da due fasi consecutive, Contenimento-Eradicazione-Ripristino e Rilevamento-Analisi ed in ultimo una fase di Analisi Post-Incidente

? Una fase di Preparazione Iniziale e poi una fase ciclica composta da due parti: Rilevamento-Analisi e Contenimento-Eradicazione-Ripristino ed in ultimo una fase di Analisi Post-Incidente

? Un ciclo composto da due fasi, Rilevamento-Analisi e Contenimento-Eradicazione-ripristino e una fase di Analisi Post-Incidente

? Una fase di Preparazione Iniziale, una fase di Rilevamento-Analisi, una fase di Contenimento-Eradicazione-Ripristino ed in ultimo una fase di Analisi Post-Incidente

? Una fase prima dell'incidente, una fase durante l'incidente e una fase dopo l'incidente

? Una fase di Rilevamento dell'Incidente e di Verifica dei danni dopo l'incidente

(M3.1.2.4) L'Action Workflow

? È un tipo di modellizzazione basata sulle attività

? È un tipo di modellizzazione basata sull'interazione o la negoziazione

? È un tipo di modellizzazione basata sui dati

? È particolarmente adatto a rappresentare processi in cui gli elementi di decisione sono particolarmente importanti

? Mette al centro del modello le condizioni di soddisfazione (o di accordo) tra un cliente e un operatore/realizzatore

? Mette al centro del modello le informazioni sulla sequenza delle attività da realizzare

(M3.1.3.5) Lo Standard Internazionale

? ISO 45001:2018 è relativo alla sicurezza del lavoro

? ISO 14001:2015 è relativo all'ambiente ovvero sui sistemi di gestione ambientale

? ISO 26000:2010 è relativo alla contabilità aziendale

? ISO 9001:2015 è relativo alla qualità

? ISO 27001:2013 è relativo alla sicurezza delle informazioni

? ISA/IEC 62443 è relativo alla sicurezza delle reti informatiche aziendali in generale

(M3.2.1.12) La macroarea "Linee Guida" della famiglia di standard ISO/IEC 27000 include le norme

? 27001

? 27003

? 27006

? 27007

? 27011

- 27021

(M3.2.1.13) La macroarea "Requisiti" della famiglia di standard ISO/IEC 27000 include le norme

- 27001
- 27006
- 27009
- 27002
- 27003
- 27011

(M3.2.1.14) Nell'ISO/IEC 27000 il ciclo di Deming o PDCA si associa

- Il PLAN alla pianificazione in un ISMS
- Il PLAN all'istituzione di un ISMS
- Il DO all'implementazione e conduzione dell'ISMS
- Il CHECK al monitoraggio e alla revisione dell'ISMS
- L'ACT all'attuazione dell'ISMS
- L'ACT alla manutenzione e al miglioramento dell'ISMS

(M3.2.1.15) Nell'area tematica di criticità "Supporto" dell'ISO/IEC 27001 sono presenti i seguenti requisiti

- Risorse
- Politica
- Consapevolezza
- Comunicazione
- Informazioni documentate
- Leadership e impegno

(M3.2.1.17) Nell'area tematica di criticità "Contesto dell'Organizzazione" dell'ISO/IEC 27001 sono presenti i seguenti requisiti

- Comprendere l'organizzazione e il suo contesto
- Comprendere le necessità e le aspettative delle parti interessate
- Comprendere le necessità di sicurezza del profilo di business
- Determinare il campo di applicazione del sistema di gestione per la sicurezza delle informazioni
- Sistema di gestione per la sicurezza delle informazioni
- Sistema di gestione della sicurezza di reti e sistemi

(M3.2.1.16) Quali delle seguenti sono Aree di Controllo secondo ISO 27001 2013?

- Politiche per la sicurezza delle informazioni

- Politiche per la sicurezza dei dati
- Sicurezza fisica e ambientale
- Sicurezza logica e fisica
- Gestione dei Fornitori
- Gestione dei clienti

(M3.2.2.1) L'Area di Controllo 7 dell'ISO 27001 2013 Annex A "Sicurezza delle Risorse Umane" include le seguenti Categorie di Controllo

- Prima dell'impiego
- Selezione del personale
- Durante l'impiego
- Formazione del Personale
- Discontinuità del rapporto di lavoro
- Cessazione e variazione del rapporto di lavoro

(M3.2.2.2) L'Area di Controllo 9 dell'ISO 27001 2013 Annex A "Controllo degli Accessi (logici)" include le seguenti Categorie di Controllo

- Requesiti di business per il controllo degli accessi
- Gestione degli accessi degli utenti
- Responsabilità dell'utente
- Responsabilità del manager
- Controllo degli accessi ai sistemi e alle applicazioni
- Controllo degli accessi fisici ai sistemi e alle applicazioni

(M3.2.3.8) Nel Framework Core di NIST CF la funzione "Identify" è costituta dalle seguenti Categorie:

- Asset management
- Business Environment
- Analysis
- Risk Mitigation
- Risk Management Strategy
- Supply Chain Risk Management

(M3.2.3.9) Nel Framework Core di NIST CF la funzione "Protect" è costituta dalle seguenti Categorie:

- Identity Management and Access Control
- Awareness and Training
- Data Security
- Information Protection Processes & Procedures

- Anomalies and Events
- Protective Technology

(M3.2.4.1) Le guide verticali NIST Special Publications sono raggruppate in:

- SP 800 Computer security
- SP 1800 Cybersecurity Practice Guides
- SP 1700 Cybersecurity Development Guides
- SP 500 Information Technology (Relevant Documents)
- SP 300 Information Technology (Relevant Documents)
- SP 600 Computer System Management

(M3.2.6.10) Ciascun elemento di un SCMS secondo l'ISA/IEC 62443 ha

- Un Obiettivo per Identificare chiaramente gli obiettivi dei requisiti dell'elemento
- Un Fondamento Logico che fornisce una guida per chiarire la logica dei requisiti dell'elemento
- Una Descrizione estesa dell'elemento e dei requisiti che sono contenuti
- Un link a documenti associati
- Associati una lista di requisiti
- Associato un solo requisito specifico

(M3.2.6.11) Quali dei seguenti sono Fondational Requirements secondo ISA/IEC 62443

- Identification and Authentication Control (IAC)
- User Controller (UCR)
- System Integrity (SI)
- Data Confidentiality (DC)
- Restrict Data Flow (RDF)
- Resource Providing (RP)

(M3.3.1.4) Perché è importante la regolamentazione GDPR per l'Information Technology?

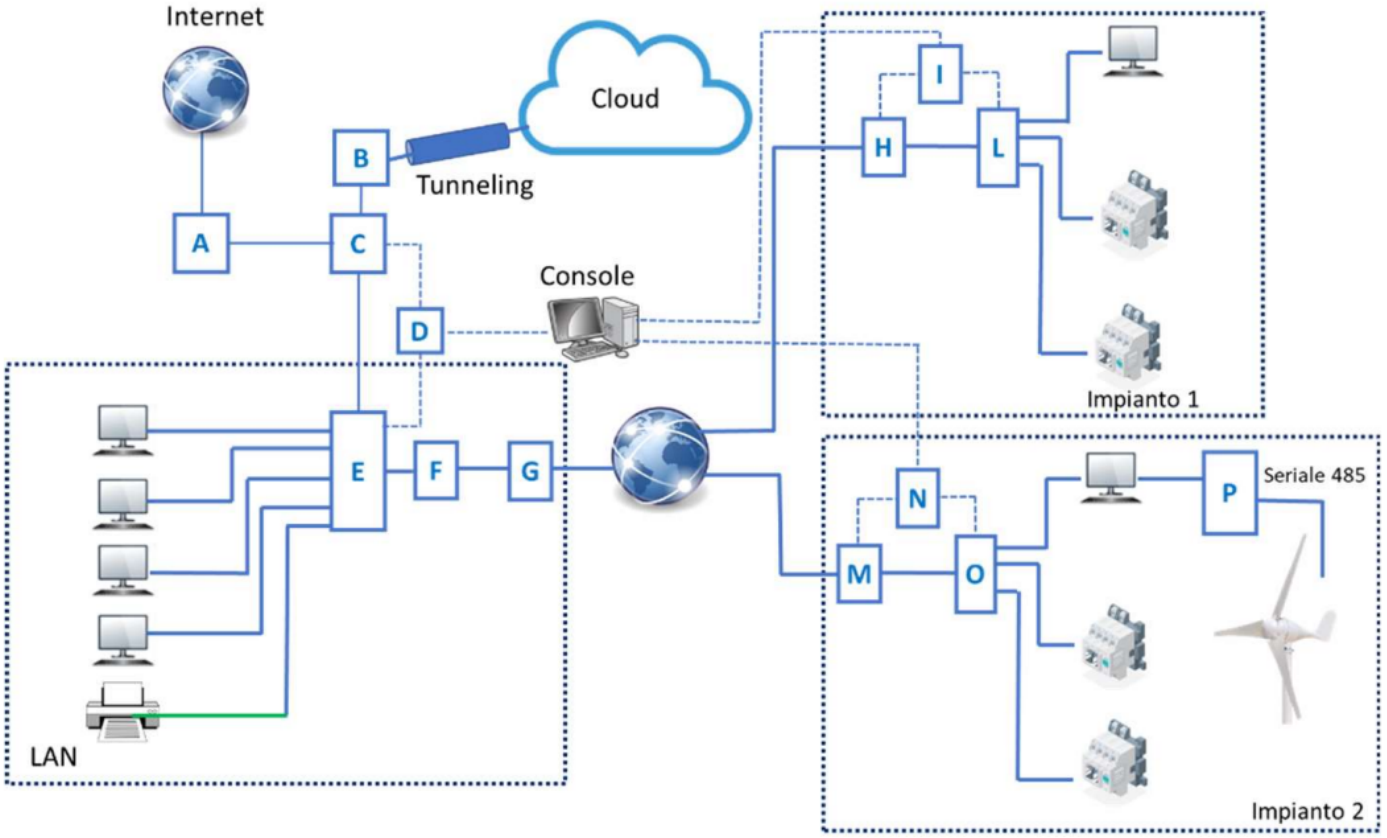
- Perché i sistemi informativi conservano, gestiscono e permettono di trasferire i dati riservati e sensibili delle persone
- Perché i dati sono archiviati e mantenuti per periodi di tempo indeterminati, potenzialmente senza possibilità di controllo dalle persone stesse
- Perché una gestione dei dati senza regole può mettere a repentaglio le regole principali del vivere civile ed è quindi necessario regolamentare la gestione dei dati nel suo insieme
- Perché una gestione dei dati senza regole può mettere a repentaglio le regole principali del vivere civile ed è quindi necessario regolamentare la gestione dei dati: ovviamente solamente l'autorizzazione al trattamento e al trasferimento

? Perché una gestione dei dati senza regole può mettere a repentaglio le regole principali del vivere civile ed è quindi necessario regolamentare la gestione dei dati: dall'autorizzazione al trattamento, il trasferimento sino al tempo massimo di mantenimento

? Perché bisogna salvaguardare gli aspetti formali del trattamento dei dati

Esercizio 1

Data la seguente topologie di rete:



Indicare la tipologia degli apparati e sistemi nei quadrati e rettangoli:

A	B	C	D	E	F	G	H	I
Router	VPN	Firewall	Anomaly Detection System	Switch	Firewall	Router	Router-Firewall	Anomaly Detection System

L	M	N	O	P
Switch	Router-Firewall	Anomaly Detection System	Switch	Gateway

Esercizio 2

Partizionare la rete 192.168.10.0 in 4 sottoreti così costituite, ogni sottorete deve essere suddivisa in due VLAN uguali. Rappresentare le sottoreti con la notazione /X ed esplicitare il numero totale degli Host della sottorete:

- Sottorete A: 68 Host
- Sottorete B: 26 Host
- Sottorete C: 12 Host

- Sottorete D: 58 Host

					VLAN	N° Totale Host
192	168	10	0	/25	1	63
192	168	10	0	/25	2	63
192	168	10	128	/27	3	15
192	168	10	128	/27	4	15
192	168	10	160	/28	5	7
192	168	10	160	/28	6	7
192	168	10	176	/26	7	31
192	168	10	176	/26	8	31

Appello 17 Febbraio 2023 - T3

(1- M1.1.4.5) L' Uniform Resource Locator (in acronimo URL)

- Identifica univocamente l'indirizzo di una risorsa su una rete di computer
- Necessita di una "risoluzione" in indirizzo IP per l'instradamento con l'analogo protocollo
- È un indirizzo composto da vari parametri che possono essere opzionali
- Può essere una sequenza alfanumerica o binaria
- In nessun caso può utilizzare un protocollo criptato
- È nato per facilitare la consultazione delle risorse on-line siano esse interi siti web, pagine HTML, foto o video

L' Hypertext Transfer Protocol (in acronimo HTTP)

- Utilizza il comando PEEK che recupera una risorsa dal server (ad es. visitando una pagina)
- Utilizza il comando POST che invia una risorsa al server (ad es. compilando un modulo)
- Utilizza il comando DELETE che cancella una risorsa dal server (ad es. eliminando un file)
- Utilizza il comando POKE che forza una determinata area di memoria (ad es. caricando un valore in un registro)
- Utilizza il comando PUT che memorizza una risorsa sul server (ad es. caricando un file)
- Utilizza il comando HEAD che recupera solo l'header della risposta senza la risorsa

(3- M1.3.2.9 - 23) Nella comunicazione con il protocollo Ethernet in caso di avvenuta collisione:

- La stazione trasmittente sospende la trasmissione e trasmette una sequenza composta dalla parte di pacchetto già trasmessa e un codice identificativo in coda al pacchetto
- La stazione trasmittente sospende la trasmissione e trasmette e un codice identificativo in testa e la parte di pacchetto già trasmessa in coda al pacchetto
- La stazione trasmittente sospende la trasmissione e trasmette una sequenza (detta di Jamming) per avvisare che il canale è occupato
- La stazione di trasmissione, dopo l'invio della sequenza di jamming, ripete il tentativo di trasmissione per un numero di volte non superiore a 5

- La stazione di trasmissione, dopo l'invio della sequenza di jamming, ripete il tentativo di trasmissione dopo un tempo pseudocasuale, per evitare la ripetizione della collisione
- La stazione trasmittente interrompe le trasmissioni e attende un segnale di Restart da parte di una altra stazione

(4- M1.3.2.12 -23) La comunicazione deterministica real-time:

- È una qualsiasi forma di comunicazione per cui gli utenti possono scambiarsi informazioni anche non nell'esatta sequenza che sono state generate ma con una latenza prevedibile o comunque predefinita
- È una qualsiasi forma di comunicazione per cui gli utenti possono scambiarsi informazioni in maniera deterministica, istantaneamente o con una latenza trascurabile o comunque predefinita
- Ha, di solito, necessità di garantire la sincronizzazione tra due o più dispostivi (es. dispositivo di comando e di attuazione)
- Deve garantire tempi di comunicazione sempre sotto il nanosecondo
- Può permette il controllo di macchinari senza una connessione meccanica
- Deve garantire tempi di trasmissione compatibili con le dinamiche dei dispositivi o i processi coinvolti

(5- M1.3.3.10) Le regole configurabili nel firewall

- Hanno tra le impostazioni di base l'indirizzo IP sorgente
- Hanno tra le impostazioni di base l'indirizzo IP di destinazione
- Hanno tra le impostazioni di base la porta attraverso la quale viene erogato il servizio
- Non possono abilitare o disabilitare solo uno specifico protocollo (Es. UPD, TCP, ecc.)
- Possono utilizzare un criterio di applicazione di tipo "Default-reject"
- Possono utilizzare un criterio di applicazione di tipo "Default-allow"

(6- M2.1.1.1-23) L'Azienda: (RIPETUTA)

- È un'organizzazione di persone e beni economici
- È un'organizzazione di persone e beni economici ma non beni strumentali
- Ha al suo interno anche beni strumentali, ovvero beni economici utilizzati per la produzione di altri beni
- Ha al suo interno solo persone e beni materiali, ovvero che hanno consistenza fisica
- Esercita l'insieme delle funzioni aziendali per il raggiungimento degli obiettivi prefissati
- Realizza l'attività aziendale attraverso i processi aziendali, nell'ambito della sua gestione operativa

(7- M2.1.2.4-23) Le aziende di produzione

- Possono essere solo le aziende che assemblano direttamente i beni o forniscono direttamente i servizi
- Hanno obiettivi primari legati alla stessa sopravvivenza dell'impresa

? Possono essere sia di produzione diretta dei beni o servizi sia di produzione indiretta ovvero che creano valore aggiunto a beni e servizi già esistenti

? Hanno come scopo quello di realizzare uno scambio con altre aziende, amministrazioni pubbliche e consumatori finali. Tale scambio ha per oggetto beni o servizi in cambio dei quali l'impresa riceve un compenso

? Hanno tra gli obiettivi solo la soddisfazione di un limitato gruppo di persone

? Non possono essere aziende di capitali

(8- M2.2.1.5) Quali strategie posso utilizzare per proteggere da un possibile attacco cyber ad una linea produttiva (al momento l'unica che produce un determinato bene)?

? Identificare e proteggere (o eliminare) eventuali connessioni dirette alla rete pubblica (internet) V

? Realizzare un adeguato sistema di segmentazione e segregazione delle reti e degli apparati di controllo

? Gestire gli accessi remoti ai sistemi informatici di linea con opportune procedure, autorizzazioni, tecnologie

? Valutare la realizzazione di una linea produttiva parallela analoga alla prima che utilizza la stessa rete

? Identificare eventuali obsolescenze software e hardware e vulnerabilità standardizzate (CVE) nei sistemi industriali

? Isolare completamente la rete industriale dalla rete office

(9- M2.2.2.5) Il vettore di attacco

? Sfrutta debolezze o vulnerabilità solamente tecnologiche

? È la tecnica di attacco unicamente diretta e frontale verso un firewall perimetrale

? Per esteso può essere la tecnica utilizzata per l'accesso non autorizzato da parte di un malintenzionato ad un dispositivo o una rete per scopi nefasti

? Può sfruttare meccanismi di autenticazione deboli

? Può sfruttare debolezze umane come mancanza di conoscenza o attenzione

? Può utilizzare e-mail di phishing, app malevole, chiavette USB infette, botnet, ecc.

(10- M2.3.1.1-23) La Gestione Aziendale

? È l'insieme coordinato di operazioni soggettive e oggettive che l'azienda compie per raggiungere gli obiettivi prefissati

? È l'insieme delle operazioni soggettive di conduzione che il manager compie per raggiungere gli obiettivi prefissati

? Realizza operazioni soggettive, ovvero le attività svolte dagli organi aziendali, decisioni e controlli, da effettuare al fine di raggiungere gli obiettivi fissati

? Definisce i piani strategici e organizzativi di lungo periodo

? Realizza operazioni oggettive e soggettive per il raggiungimento della soddisfazione del cliente e dei fornitori

- Si caratterizza in operazioni di: acquisizione dei mezzi monetari, acquisizione di fattori produttivi col capitale monetario e trasformazione di fattori in prodotti o servizi finiti

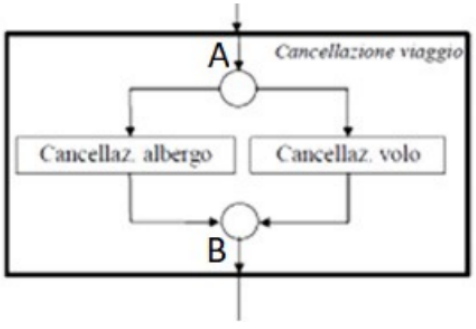
(11- M2.3.2.1-23) I Processi Aziendali

- Possono essere definiti come un insieme di attività, non necessariamente collegate, che possono portare a diversi obiettivi a carattere strategico
- Possono essere definiti come un insieme di attività interdipendenti, svolte all'interno dell'azienda che creano valore trasformando delle risorse in un prodotto o servizio finale a valore aggiunto
- Devono prevedere un solo input chiaramente definito e più risultati finali
- Devono prevedere input, chiaramente ben definiti, e un singolo risultato finale
- Hanno input che sono costituiti da tutti i fattori che contribuiscono (direttamente e indirettamente) al valore aggiunto di un servizio o di un prodotto
- I processi si possono modellizzare attraverso l'uso dei diagrammi di flusso

(12- M3.1.1.2) L'Incident Response Plan (Piano di risposta agli incidenti)

- Permette di rispondere ad un attacco esterno mediante misure controffensive verso l'attaccante
- Permette di rispondere all'esigenza di individuare gli attacchi e mitigare il danno
- Esegue anche la post analysis che consente di delineare la reale portata dell'incidente
- È un insieme di procedure documentate che descrivono in dettaglio i passaggi da intraprendere in ciascuna fase della risposta agli incidenti
- Se ben strutturato e documentato può non essere aggiornato frequentemente
- Dovrebbe includere linee guida per ruoli e responsabilità, piani di comunicazione e processi di risposta standardizzati

(13- M3.1.2.1-23) Nella Business Transaction rappresentata utilizzando il modello WIDE qui sotto:



- Una volta entrati per il punto A i task Cancellazione Albergo e Cancellazione Volo vengono eseguiti contemporaneamente
- Una volta Entrati per il punto A i task Cancellazione Albergo e Cancellazione Volo vengono eseguiti uno successivo all'altro (terminato Cancellazione Albergo viene eseguito Cancellazione Volo)
- Si giunge al punto B solo dopo che entrambi i task Cancellazione Albergo e Cancellazione Volo sono stati eseguiti completamente
- Si giunge al punto B anche se nessuno tra i task Cancellazione Albergo e Cancellazione Volo è stato eseguito completamente

? Si giunge al punto B solo se i task Cancellazione Albergo e Cancellazione Volo si concludono contemporaneamente

? Il punto B può anche non essere mai raggiunto

(15- M3.2.1.20) Cos'è un ISMS secondo ISO 27001

? Un insieme di regole che un'azienda deve stabilire per gestire la sicurezza delle informazioni

? Un insieme di regole che, tra le altre cose, permettano di identificare gli stakeholder e le loro aspettative in termini di sicurezza delle informazioni

? Un insieme di regole che, tra le altre cose, permettano di identificare quali rischi fisici esistano per le persone

? Un insieme di regole che, tra le altre cose, permettano di definire i controlli e altri metodi di mitigazione per soddisfare le aspettative identificate e gestire i rischi

? Un insieme di regole che, tra le altre cose, permettano di fissare obiettivi chiari su ciò che deve essere raggiunto con la sicurezza delle informazioni

? Un insieme di regole che, tra le altre cose, permettano di attuare tutte le contromisure e gli altri metodi per il trattamento dei vincoli di tipo normativo

(16- M3.2.1.6-23) Quali delle seguenti sono Aree di Controllo secondo ISO 27001 2013?

? Gestione dei Fornitori

? Organizzazione della sicurezza delle informazioni

? Sicurezza dei sistemi negli impianti di produzione

? Gestione dell'infrastruttura di rete

? Aspetti di sicurezza per la gestione della Business Continuity

? Crittometria

(17- M3.2.1.9-23) Secondo ISO 27002 2013 una Categoria di Controllo è:

? Il controllo stesso

? È la dichiarazione estesa dell'obiettivo che si vuole raggiungere

? È di fatto l'Area del Controllo

? È l'appropriata contromisura in esame

? È la descrizione della finalità dello specifico controllo

? Uno dei tre livelli dello schema con cui sono strutturati i controlli

(19- M3.2.3.10) Nel NIST CSF Core le sottocategorie

? Le sottocategorie dividono ulteriormente una Categoria in risultati ottenibili avendo intrapreso attività tecniche e/o gestionali

? Forniscono una serie di risultati che, sebbene non esaustivi, aiutano a supportare il raggiungimento dei risultati in ciascuna categoria

? Non hanno mai associato nessun Riferimento Normativo

? Un esempio di sottocategoria può includere "I sistemi di informazione esterni sono catalogati"

? Un esempio di sottocategoria può includere "Selezionare quali dati da proteggere"

? Un esempio di sottocategoria può includere "Le notifiche dai sistemi di rilevamento vengono esaminate"

(22- M3.2.6.6-23) I Foundational Requirements secondo ISA/IEC 62443

? Sono stati definiti dal momento che il classico modello CIA (Confidentiality, Integrity e Availability) non si adatta interamente ai requisiti richiesti per gli IACS (Industrial Automation and Control Systems)

? Sono stati definiti dal momento che il classico modello CIA (Confidentiality, Integrity e Availability) si adatta ai requisiti industriali necessari per il funzionamento degli apparati sulle reti OT

? Sono sette requisiti di base

? Sono quattordici requisiti di base

? Sono otto requisiti di base

? Focalizzano gli aspetti di cyber sicurezza in relazione al funzionamento degli IACS

(23- M3.2.6.13) Gli IACS secondo l'IEC 62443?

? Sono gli Industrial Automation and Control Systems ovvero i sistemi di controllo e di automazione industriali

? Possono essere gli SCADA (Supervisory Control and Data Acquisition) ovvero i sistemi di supervisione e acquisizione dati

? Possono essere le telecamere del sistema perimetrale di sicurezza

? Possono essere i PLC (Programmable Logic Controller) ovvero i sistemi di controllo a logica programmabile

? Possono essere i DCS (Distributed control system) ovvero i sistemi di Controllo Distribuito di processo

? Possono essere gli strumenti di analisi della produzione presenti nella rete office

(25- M3.3.7.3) Quali delle seguenti sono caratteristiche della certificazione di cybersicurezza secondo il Regolamento (UE) 2019/881:

? Protezione dei dati dalla distruzione o dall'alterazione accidentale o non autorizzata

? Accesso garantito a tutti i dati, ai servizi o alle funzioni senza discontinuità operativa

? Nessuna registrazione storica degli accessi a dati, servizi o funzioni

? Ripristino tempestivo dell'accesso ai dati, ai servizi o alle funzioni in caso di incidente

? Utilizzo di criteri di security by design per la progettazione

? Aggiornamento costante di software e hardware

(26- M3.4.3.2-23) Il Rischio Informatico può essere valutato come

? Impatto x Probabilità

? Impatto elevato alla Probabilità

- Impatto x Frequenza
- Un numero compreso tra un valore minimo e uno massimo in funzione dell'incertezza del rischio
- Un numero sempre compreso tra 1 (Rischio Molto Basso) e 4 (Rischio Molto Alto) in funzione dell'incertezza del rischio
- Un numero che è funzione dell'incertezza e fa riferimento a classi omogenee di eventi, per natura e gravità

(27- M3.4.1.2) Perché la leadership aziendale è fondamentale per la definizione di un SGSI (Sistema di Gestione della Sicurezza Informatica)?

- Perché altrimenti possono non essere garantiti gli investimenti necessari per la sua realizzazione
- Perché senza il benestare chiaro, motivato e comunicato della leadership aziendale non si riuscirà a coinvolgere efficacemente tutto il personale aziendale
- Perché altrimenti non si riusciranno a portare a termine i cambiamenti nelle politiche, nei processi e nelle procedure necessari
- Perché solo una leadership consapevole può capire sino in fondo l'impatto possibile della sicurezza informatica con il funzionamento dell'organizzazione
- Così è chiara la responsabilità in caso di cattivo funzionamento del sistema di gestione
- Così è possibile creare nuove figure e ruoli che altrimenti sarebbe impossibile definire

(28-M4.2.2.3) Quali dei seguenti elementi possono migliorare la percezione del rischio cyber da parte dei dipendenti aziendali

- La formazione e sensibilizzazione continua dei dipendenti per renderli consapevoli delle minacce cyber
- L'educazione dei dipendenti in merito alle policy e procedure già definite dall'organizzazione ma che non vengono rispettate adeguatamente
- La maggiore dotazione di dispositivi elettronici per semplificare le operazioni dei dipendenti
- L'innalzamento del livello di sicurezza e di notifica dei dispositivi informatici in dotazione
- Il maggior uso di sistemi as a service che utilizzano programmi in Cloud
- Cercare di limitare le azioni ripetitive e automatiche sulle interfacce informatiche attraverso l'introduzione di blocchi che permettano una maggiore consapevolezza dell'azione che si sta realizzando

(29 – M4.2.1.2) L'organizzazione della Cybersicurezza in ambito bancario

- Ha tradizionalmente sviluppato strategie fortemente focalizzate sulla gestione del rischio
- Tradizionalmente si occupa poco degli aspetti di sicurezza logica perché tali aspetti non possono avere impatto sull'andamento finanziario dell'azienda
- Gestisce tipicamente le nuove minacce attraverso comitati di direzione per la gestione del rischio che rispondono all'amministratore delegato o al consiglio di amministrazione
- In molti casi prevede che la figura del CSO (Chief of Security Officer) abbia responsabilità anche sulla sicurezza logica della banca
- In nessun caso la figura del CSO ha responsabilità anche sulla sicurezza logica della banca

❔ Nei casi in cui il CISO (Chief Information Security Officer) non sia gerarchicamente subordinato al CSO le azioni sono da lui coordinate anche indirettamente

(30- M4.3.3.1) Nell'organigramma apicale di una grande multiutility

❔ L'Information Technology è di solito collocata nell'area di responsabilità della direzione dell'innovazione o della direzione tecnica o tecnologica

❔ L'Information Technology di solito risponde al vicepresidente esecutivo

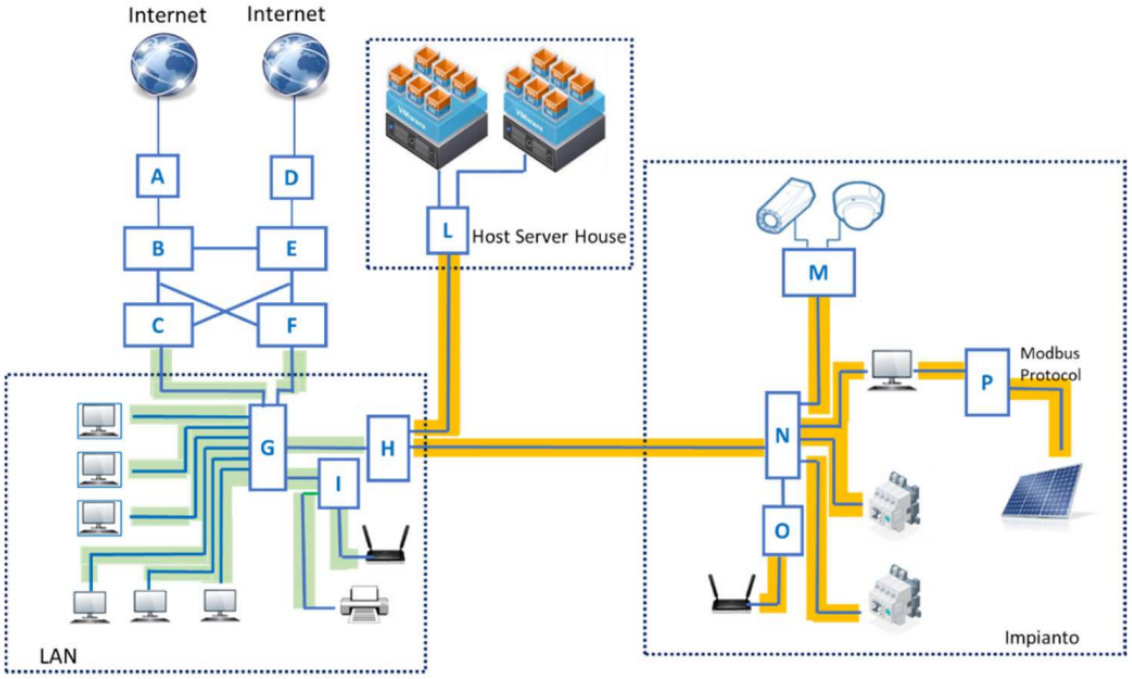
❔ La sicurezza informatica di solito riceve input dalla direzione o dai comitati che si occupano di risk management

❔ In nessun caso il CISO risponde direttamente al CEO

❔ Il CISO (o figura equivalente) di solito risponde al responsabile/direttore dei sistemi informativi (CIO o equivalente)

❔ Il CISO (o figura equivalente) non risponde mai al responsabile/direttore dei sistemi informativi (CIO o equivalente)

Esercizio 1

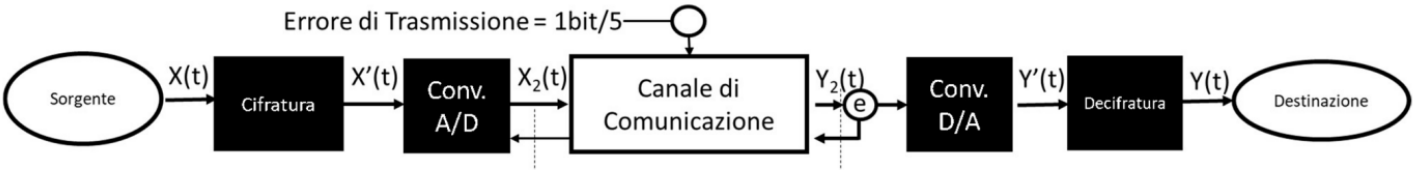


A	B	C	D	E	F	G	H	I
Router	Firewall	Switch	Router	Firewall	Switch	Switch	Firewall	Switch
L	M	N	O	P	Q			
Switch	Switch	Switch	Switch	Gateway	Conduit			

Esercizio 2

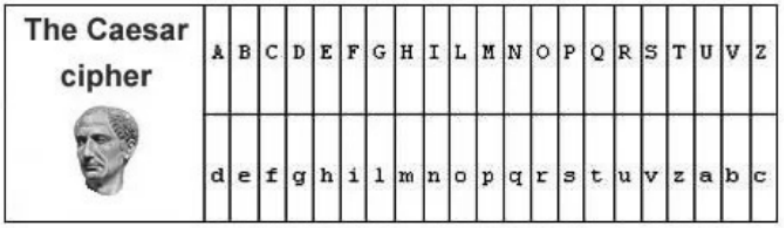
Nel canale di comunicazione criptato con cifratura a traslazione 4 che utilizza codifica binaria a 5 bit (00000=A), con alfabeto inglese, e un codice di errore ad un bit (bit di parità pari), con errore casuale massimo di un bit su venti.

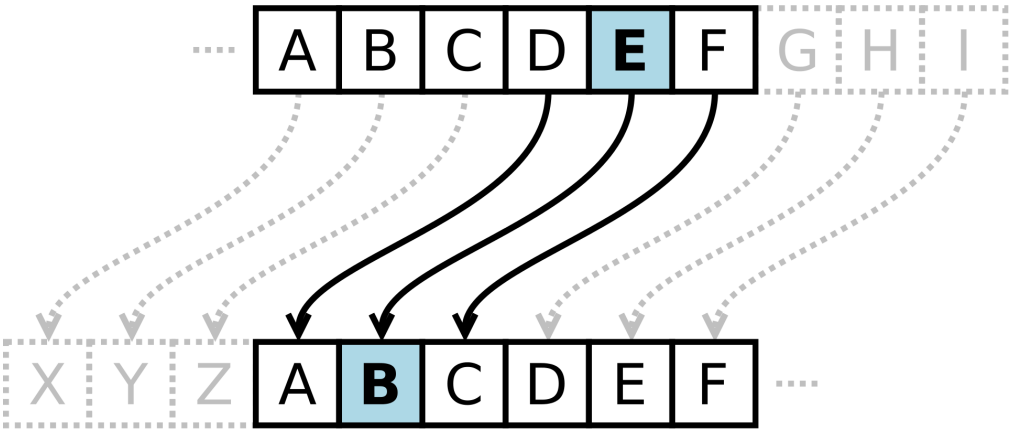
Rappresentare la stringa di bit 21 bit X2(t), con bit di parità pari e il segnale ricevuto senza errore Y2(t) e con errore di un bit Y2e(t) nel caso della trasmissione della parola “CANE”



$X_2(t)$ =	0	0	1	0	1	0	0	0	1	1	1	0	0	0	0	0	0	1	1	1	0
$Y_2(t)$=	0	0	1	0	1	0	0	0	1	1	1	0	0	0	0	0	0	1	1	1	0
$Y_{2e}(t)$=	0	0	1	0	1	0	0	0	1	1	1	0	0	0	0	0	0	1	1	1	0

Una inversione (1-0, 0-1) qualunque in uno dei bit indicati





Appello 7 Luglio 2023 - T2

Le reti telefoniche cellulari:

- ? Sono di fatto reti di comunicazione wireless
- ? Derivano il proprio nome dalla cella (o cubicolo) dove sono installati gli apparati elettronici
- ? Derivano il proprio nome dalle celle, porzioni di territorio con stazioni radio fisse, a cui si collegano gli apparati mobili
- ? Utilizzano canali di trasmissione con frequenze differenti tra celle adiacenti
- ? A causa del grosso frazionamento sul territorio hanno bisogno di un'elevata potenza di trasmissione
- ? Scambiano continuamente segnali con gli apparati mobili per migliorare la qualità di trasmissione

(M1.1.3.1.1) Nel Packet Switching (la tecnica di commutazione): (RIPETUTA)

- ? Il messaggio viene diviso in parti più piccole (packets) che vengono gestite singolarmente
- ? I messaggi vengono raggruppati in pacchetti (packets) che vengono trasmessi insieme
- ? Ai pacchetti (packets) viene assegnato nell'intestazione Indirizzo Sorgente, la Destinazione ed altri dati
- ? I pacchetti viaggiano attraverso la rete, prendendo il percorso più breve possibile (routing)
- ? I pacchetti vengono suddivisi e trasmessi in maniera indipendente e riassemblati all'estremità ricevente nell'ordine di arrivo
- ? Se un messaggio arriva mancante di pacchetti o danneggiato verrà inviata una notifica per inviare nuovamente il messaggio, se invece viene raggiunto l'ordine corretto dei pacchetti, verrà inviata notifica di conferma

(M1.2.4.3.2) Il Furto di Identità Digitale

- ? È punito dal Codice Penale Italiano come "Sostituzione della propria all'altrui persona" e "Frode Informatica"
- ? Può essere associato al solo reato di "Truffa"
- ? Può avvenire mediante operazioni di Phishing
- ? È relativo all'uso illecito dell'insieme dei dati e delle informazioni che definiscono un individuo e costituiscono la rappresentazione virtuale dell'identità reale utilizzabile durante interazioni elettroniche
- ? È relativo ai soli dati biometrici che definiscono un individuo e costituiscono una delle rappresentazioni virtuali dell'identità reale utilizzabile durante interazioni elettroniche
- ? È un reato amministrativo secondo l'ordinamento italiano

(M1.2.4.9.1) L'Advanced Persistent Threat (APT)

- È una minaccia perpetrata da un avversario dotato di notevole bagaglio tecnico e grandi risorse, in grado di effettuare attacchi su vasta scala, utilizzando molteplici vettori, e per periodi di tempo molto estesi
- È una minaccia che colpisce aziende molto grandi
- È di solito gestita da gruppi organizzati e/o da stati sovrani
- Utilizza software pubblicamente disponibili per riuscire meglio a propagarsi
- Può utilizzare software creati ad hoc, più versatili e complessi da rilevare
- Per raccogliere informazioni sui propri obiettivi può utilizzare tool estremamente sofisticati, e, potenzialmente, anche appoggiarsi ai servizi di intelligence del paese di provenienza

(M1.3.1.24.1) Il livello 1 del Modello ISO/OSI

- Converte i bit in un pacchetto in un segnale fisico per il mezzo di trasmissione
- Ha tra le funzioni l'adeguamento elettrico degli apparati trasmissivi
- Può utilizzare protocolli Bluetooth
- Può utilizzare il protocollo IP
- È l'interfaccia tra software e hardware nello stack ISO/OSI
- Vincola i livelli superiori agli specifici mezzi fisici di comunicazione

(M1.3.2.14.1) I protocolli seriali multipunto

- Sono protocolli seriali punto-punto che possono collegare ulteriori unità attraverso una connessione multi-drop
- Possono utilizzare lo standard RS-422 e RS-485
- In una configurazione con molte unità connesse solo un paio possono effettivamente comunicare
- Possono utilizzare lo standard Bluetooth
- Sia nel caso di RS-422 che di RS-485 possono essere contemporaneamente bidirezionali
- Solo nel caso dello standard RS-422 possono essere contemporaneamente bidirezionali

(M1.3.2_2.5) Il modello di comunicazione Broadcast:

- Identifica la comunicazione uno a tutti
- Identifica la comunicazione ad ampio spettro, uno a ad alcuni
- Può avvenire a livello 2 dello stack ISO (indirizzamento MAC)
- Può avvenire a livello 3 dello stack ISO (Indirizzamento IP)
- Può peggiorare la latenza nella rete
- Può migliorare la latenza di rete

(M1.3.2_2.6) La subnet 160.12.32.128/19

- Ha come indirizzo di rete 160.12.32.0
- Ha come indirizzo di broadcast 160.12.63.255
- Ha come indirizzo di broadcast 160.12.63.64
- Ha come maschera di sottorete 255.255.224.0
- Ha come maschera di sottorete 255.255.32.0
- Lo spazio di indirizzamento arriva sino a (HostMax) 160.12.63.254

(M1.3.2_2.7) La subnet 160.12.32.128/20

- Ha 4.096 indirizzamenti disponibili
- Può connettere 4.094 hosts
- Ha 220 (1.048.576) indirizzamenti possibili
- Ha un numero di indirizzamenti possibili maggiore di quelli della subnet 60.12.32.128/19
- Ha una maschera di rete composta da 20 bit, i più significativi, a 1
- Ha una maschera di rete composta da 12 bit, i più significativi, a 1

(M1.3.2.15.1) Lo standard elettrico RJ45

- Prevede un cablaggio con 8 fili
- Prevede un cablaggio con 10 fili
- Prevede varie categorie da 100 Mbps sino a 10 Gbps
- Prevede varie categorie da 100 Mbps sino a 100 Gbps
- Permette la connessione di un numero massimo di 4 dispositivi
- Può gestire comunicazioni multipunto per distanze superiori ai 100m

(M1.3.2.17) La modalità di trasmissione Half-Duplex

- È un tipo di modalità di comunicazione che supporta la comunicazione a due vie ma con ritardo
- È un tipo di modalità di comunicazione in cui i dati possono viaggiare solo in una direzione alla volta
- Ha come esempio della modalità di funzionamento la comunicazione tramite Walkie-Talkie
- Prevede due cavi uno per la trasmissione e uno per la ricezione
- Prevede un solo cavo per la trasmissione e ricezione
- È più efficiente della modalità Full-Duplex

(M1.3.3.6.2) Lo Switch di rete:

- È un dispositivo elettronico intelligente, dotato di porte di interfaccia di varie tipologie
- Può essere un dispositivo elettrico non dotato di CPU e, se “Unmanaged”, configurabile
- Può segmentare il dominio di broadcast attraverso le VLAN
- Può avere una gestione “Unmanaged” o “Managed”
- Può avere un instradamento “store-and-forward”
- Se “Unmanaged” non permette la configurazione delle VLAN

(M1.3.3.9) Il Firewall:

- Monitora il traffico in entrata e in uscita attraverso regole di sicurezza configurabili per autorizzare o bloccare gli eventi
- È un dispositivo, esclusivamente implementato su speciali appliance, per la sicurezza della rete
- Se NGFW (Next Generation Firewall) è dotato di funzioni di prevenzione delle intrusioni (IPS) e di funzionalità di prevenzione delle minacce e protezione antivirus
- È un dispositivo che funziona solo a livello ISO/OSI 4

(M1.3.3.7.1) Il Gateway

- È un dispositivo hardware che funge da raccordo tra due reti, solitamente una rete remota e quella che la ospita
- È un convertitore di protocolli di rete, capace di unire due reti in modo che i dispositivi presenti su un dato network possano comunicare con quelli presenti in un altro
- Può essere realizzato da: Un router, un server, un firewall, ecc.
- Di solito non converte mai protocolli di rete
- Può realizzare la funzionalità NAT (Network Address Translation)
- Differentemente dal router ha il compito di gestire un traffico simile e connettere dispositivi che condividono un’interfaccia comune

Quanti sono i rami di una topologia di rete a Maglia Completa?

- N*(N-1)/2
- N/2*(N-1)

(M1.3.4.8) Una rete peer to peer

- Ha nodi che, diversamente dalla rete client-server, possono richiedere e fornire servizi
- Ha nodi che, analogamente alla rete client-server, condividono lo stesso network
- Ha nodi che, diversamente dalla rete client-server, sono specializzati per richiedere o fornire servizi
- Può essere considerata come una rete logica da “pari” a “pari”
- È un’architettura “fisica”
- È un’architettura “logica”

(M2.1.1.5) Quali dei seguenti elementi (o funzioni aziendali) sono di solito interni ad un'azienda:

- Risorse Umane (HR)
- Produzione
- Vendite
- Fornitura materie prime
- Marketing
- Servizio Cloud

(M2.1.2.10) La Società S.r.l.

- È una società in cui i soci rispondono delle obbligazioni sociali anche oltre i limiti di quanto hanno conferito
- È una società di capitali le cui partecipazioni sono rappresentate da quote e non da azioni
- È una società in cui per le obbligazioni sociali risponde solo la società stessa con il suo patrimonio
- Sono Società a responsabilità limitata dell'imprenditore
- Sono Società a responsabilità dei soci limitata al capitale sottoscritto
- Sono Società a responsabilità dei soci illimitata oltre al capitale sottoscritto

(M2.2.2.4.1) Il Sistema Informativo aziendale l'ERP (Enterprise Resource Planning)

- È una piattaforma software che raggruppa i sistemi del reparto amministrativo, delle vendite, del magazzino e la logistica
- Permette che i dati provenienti da molteplici parti dell'azienda vengono raccolti e gestiti in maniera centralizzata
- Può gestire l'invio dei dettagli relativi alla realizzazione di un prodotto verso i sistemi produttivi
- Può gestire l'inventario dei materiali, le scorte e la movimentazione delle merci
- Permette di progettare o simulare il funzionamento di un determinato oggetto meccanico
- Può essere costituito da una piattaforma SaaS in Cloud

(M2.3.2.5/23) L'Organizzazione Aziendale

- Può essere definita come l'insieme dei processi, dei materiali, degli strumenti e delle persone che li operano e li gestiscono, in maniera coordinata, per il raggiungimento di uno scopo comune o un obiettivo di impresa
- Può essere considerata come la "struttura amministrativa" di un'azienda
- Può essere considerati l'insieme degli elementi che permettono la funzione produttiva di un'azienda
- Ha come elementi fondanti: gli obiettivi, l'assegnazione dei compiti e dei ruoli e la tecnologia che realizza la struttura produttiva
- Definisce come siano suddivise le attività fra le persone coinvolte e i meccanismi di coordinamento
- È l'insieme delle procedure operative aziendali

(M3.1.1.2.2) L'Incident Response Plan (Piano di risposta agli incidenti) può essere composto da:

- Una fase di rilevamento dell'incidente (Detect)
- La Riproduzione dell'incidente rilevato (Response)
- La Mitigazione degli effetti dell'incidente (Mitigation)
- La Registrazione dell'evento (Reporting)
- Il ripristino del sistema colpito (Recovery)
- L'investigazione sul problema che ha portato all'incidente (Remediation)

(M3.2.1.20) Quali delle seguenti sono aree tematiche dei requisiti di un ISMS secondo ISO/IEC 27001:2022?

- Context of the organization (Comprensione del contesto dell'organizzazione)
- Leadership (Leadership, coinvolgimento e focalizzazione del top management su CS)
- Planning (Corretta pianificazione delle operations di CS)
- Supporto Tecnico (Disponibilità del reparto tecnico di supporto)
- Operation (Attività operative: pianificazione e controllo, valutazione del rischio…)
- Performance Evaluation (Monitoraggio e Audit delle prestazioni di CS)

(M3.2.1.18/23) Un ISMS per ISO/IEC 27000 è un insieme di regole che un'azienda deve stabilire per:

- Identificare gli stakeholder e le loro aspettative nei confronti dell'azienda in termini di sicurezza delle informazioni
- Identificare quali rischi logici e fisici esistono per le persone all'interno dell'organizzazione
- Definire i controlli e altri metodi di mitigazione per soddisfare le aspettative (al punto 1) identificate e gestire i rischi
- Fissare obiettivi qualitativi e generici su ciò che deve essere raggiunto con la sicurezza delle informazioni
- Misurare continuamente che i controlli implementati siano effettivamente efficaci
- Migliorare continuativamente la postura dell'organizzazione relativamente alle problematiche di Cybersecurity

(M3.2.1_2.5) I nuovi controlli di ISO 27001 Rev. 2022 sono specializzati per:

- Una maggior sicurezza nella gestione dei servizi Cloud
- Preparazione dell'ICT in relazione alle problematiche di Business Continuity
- L'utilizzo prevalente di software di prodotto solo da determinati fornitori
- Migliore protezione dei dati anche in relazione del loro trattamento in funzione del GDPR
- Il miglioramento dell'Internet Browsing attraverso l'uso del filtraggio dei siti
- Lo sviluppo sicuro del codice software

(M3.2.1_2.6) I controlli ISO 27001 nella Rev. 2022 sono raccolti nei seguenti gruppi:

- Le persone
- I fornitori
- Gli oggetti fisici
- La tecnologia
- Gli aspetti organizzativi
- La Supply Chain

(M3.2.1_2.7) Nella revisione 2022 del documento ISO 27001:

- Il nuovo nome è: “Information security, cybersecurity and breach protection-Information security management systems Requirements”
- l nuovo nome è: “Information security, cybersecurity and privacy protection-Information security management systemsRequirements”
- Un certo numero di controlli è rimasto invariato
- Molti controlli sono stati accorpati
- Nessun controllo è effettivamente nuovo
- Oltre il 50% di controlli sono nuovi

(M3.2.3.2.1) Nel NIST CSF il Framework Core (RIPETUTO)

- È un insieme di attività di sicurezza informatica, effetti desiderati e riferimenti applicabili comuni a tutti i settori delle infrastrutture critiche ma anche per le altre organizzazioni
- Presenta standard, linee guida e pratiche del settore che consentono la comunicazione di attività e risultati inerenti alla sicurezza anche fisica in tutta l'organizzazione
- È costituito da cinque funzioni concorrenti e continue: Identifica, Reagisci, Rileva, Rispondi, Recupera
- È costituito da quattro funzioni concorrenti e continue: Identifica, Proteggi, Rileva, Rispondi
- Identifica le categorie e le sottocategorie chiave associate a ciascuna funzione e le abbina a riferimenti informativi di esempio come standard, linee guida e pratiche esistenti per ciascuna sottocategoria
- Associa a ciascuna funzione le categorie ovvero le suddivisioni di una funzione in gruppi di risultati di sicurezza informatica strettamente legati alle esigenze programmatiche e ad attività particolari

(M3.2.3.7.1) Nel NIST CSF il Supply Chain Risk Management (SCRM) (RIPETUTA)

- Affronta sia l'effetto di sicurezza informatica che un'organizzazione ha sulle parti esterne sia l'effetto di sicurezza informatica che le parti esterne hanno su un'organizzazione
- Può includere le attività di determinazione dei requisiti di sicurezza informatica per i fornitori
- Può includere le attività di attuazione dei requisiti di sicurezza informatica attraverso accordi formali (ad es. contratti)
- È l'insieme delle attività necessarie per gestire il rischio di sicurezza informatica associato solamente ai fornitori
- Può includere le attività di verifica che i requisiti di sicurezza informatica dei fornitori siano soddisfatti attraverso una varietà di metodologie di valutazione
- Può includere le attività di comunicazione ai fornitori di come saranno verificati e convalidati i requisiti di sicurezza fisica

(M3.2.4.3.1) Il documento NIST Special Publication SP 800-82 Rev. 2

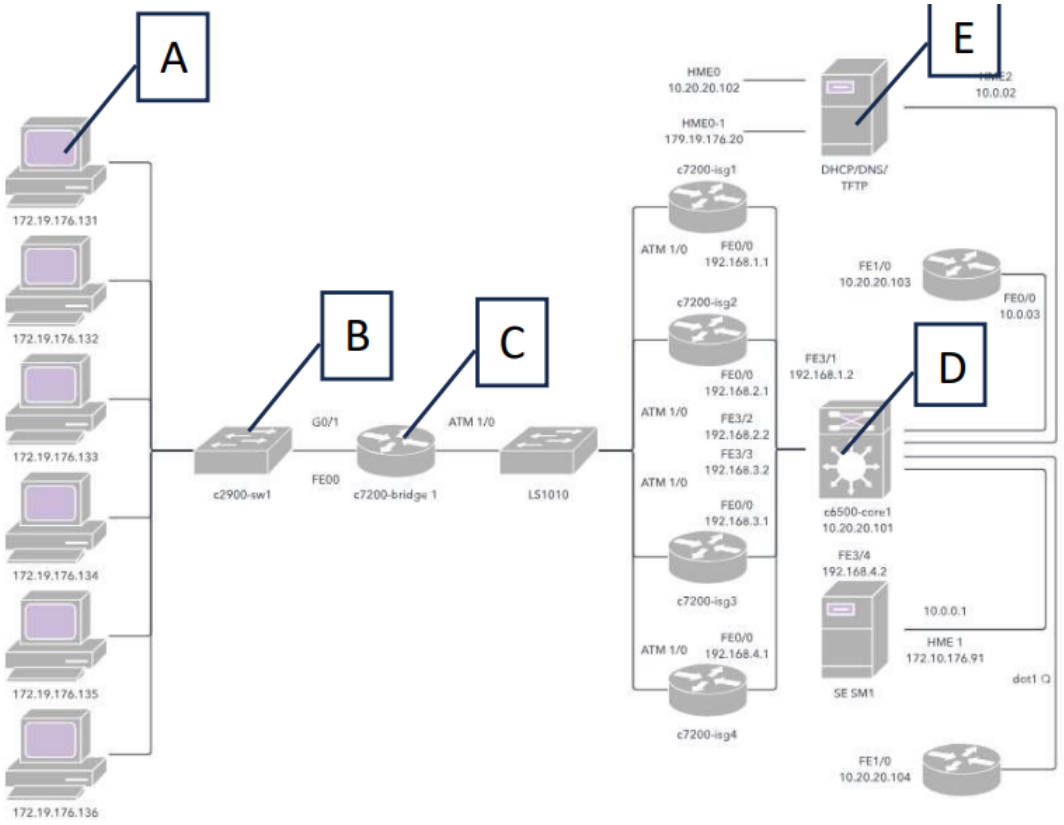
- Fornisce una guida su come proteggere i sistemi di controllo industriale (ICS)
- Fornisce un catalogo integrativo di controlli di sicurezza e privacy per i sistemi informativi e le organizzazioni
- Fa parte della serie di pubblicazioni speciali relative alla computer security
- Fa parte della serie di pubblicazioni speciali che propongono guide pratiche e usabili di soluzioni per la cybersecurity
- Fa parte della serie di pubblicazioni che sono documenti rilevanti di Information Technology
- Come tutti i documenti NIST può essere solamente acquistato nell’apposito sito

(M3.2.6.13) Il PLC (Programmable Logic Controller)

- È un sistema di controllo a logica programmabile utilizzato per le sue caratteristiche real-time
- Si interfaccia attraverso gli I/O con motori/attuatori e sensori a macchine e impianti permettendo di realizzare logiche di automazione
- Utilizza tipicamente sistemi operativi standard come, ad esempio MS Windows
- Utilizza tipicamente sistemi operativi con caratteristiche real-time o estensioni che permettano il determinismo
- Non è mai collegabile a internet
- Non ha mai problematiche di sicurezza informatica

Esercizio 1

Dato il seguente schema topologico:



Inserire negli appositi spazi i nomi dei dispositivi etichettati con le lettere:

A= Client, B=Switch, C=Router, D=Switch con funzionalità di Routing, E=Server

Esercizio 2

L'amministratore di una rete aziendale con indirizzo 128.8.0.0/16 desidera regolare l'accesso bidirezionale da Internet alla rete aziendale consentendo l'accesso dalla rete 100.10.0.0/16 (collaboratori esterni abilitati) alla sottorete interna 128.8.12.0/24 ed impedire alle sottoreti 100.10.10.0/24 e 100.10.20.0/24 (collaboratori non abilitati) di poter accedere alla stessa sottorete interna 128.8.12.0/24, indicare le regole del firewall:

Indice	IP Sorgente	IP Destinatario	Azione
1	100.10.10.0/24	128.8.12.0/24	Blocca
2	100.10.20.0/24	128.8.12.0/24	Blocca
3	100.10.0.0/16	128.8.12.0/24	Consenti
4	0.0.0.0/0	0.0.0.0/0	Blocca

Appello 7 Luglio 2023 - T2

(M1.1.4.5) La riga di testo nel linguaggio HTML:

- ❔ Identifica dove è posizionato il testo nella pagina visualizzata dal browser
- ❔ Identifica che il testo contenuto nei due comandi (di inizio e fine) è il titolo della pagina che sarà visualizzata
- ❔ Identifica che il testo contenuto sarà visualizzato con un formato grafico di tipo “title”
- ❔ Deve essere preceduta e seguita da altri comandi HTML di testo
- ❔ Può essere solo preceduta da altri comandi HTML di testo
- ❔ Può funzionare solo se attivata da un browser

(M1.1.4.1/23) L’HyperText Transfer Protocol (HTTP)

- ❔ Permette la comunicazione tra il client, ovvero il browser, ed il server, la macchina su cui risiede il sito web
- ❔ È un protocollo di livello 6 dello stack ISO/OSI
- ❔ Ha come caratteristica peculiare che terminato lo scambio di messaggi la connessione si sgancia, rendendo il protocollo molto flessibile e dinamico
- ❔ Esiste anche la versione criptata HTTPS
- ❔ Dispone di comandi, i più comuni sono: Get, Head, Post, Put, Delete
- ❔ Di “default” utilizza la porta 60 per la comunicazione da client a host (server)

(M1.2.2.2) Il Deep Web

- ❔ È quella la parte di web che non è indicizzata dai motori di ricerca
- ❔ Si considerano, di solito, siti privati, interni aziendali, accademici o di ricerca
- ❔ Possono contenere informazioni riservate, strategiche o estremamente sensibili
- ❔ Si può accedere solamente mediante specifici browsers, determinate configurazioni e accessi autorizzativi
- ❔ Si può accedere conoscendo l’indirizzo URL dello specifico sito
- ❔ È di solito il territorio della criminalità organizzata

(M1.2.3.3.1) Un attacco cyber alla Supply Chain

- Può essere diretto ad un'azienda produttrice che rifornisce un'azienda bersaglio dell'attacco
- Può essere realizzato mediante del codice software malevolo realizzato (anche involontariamente) da un consulente esterno
- Può essere una conseguenza dell'internalizzazione delle attività di sviluppo del software
- Può essere vettorizzato dal fornitore di servizi Cloud
- Di solito rivela una postura di cybersicurezza peggiore del bersaglio rispetto al fornitore, origine del vettore d'attacco
- Può mirare non solamente alla disponibilità del sistema informativo del bersaglio ma anche al blocco o rallentamento della produzione dello stesso

(M1.3.2_2.6*) La subnet 160.12.32.100/18:

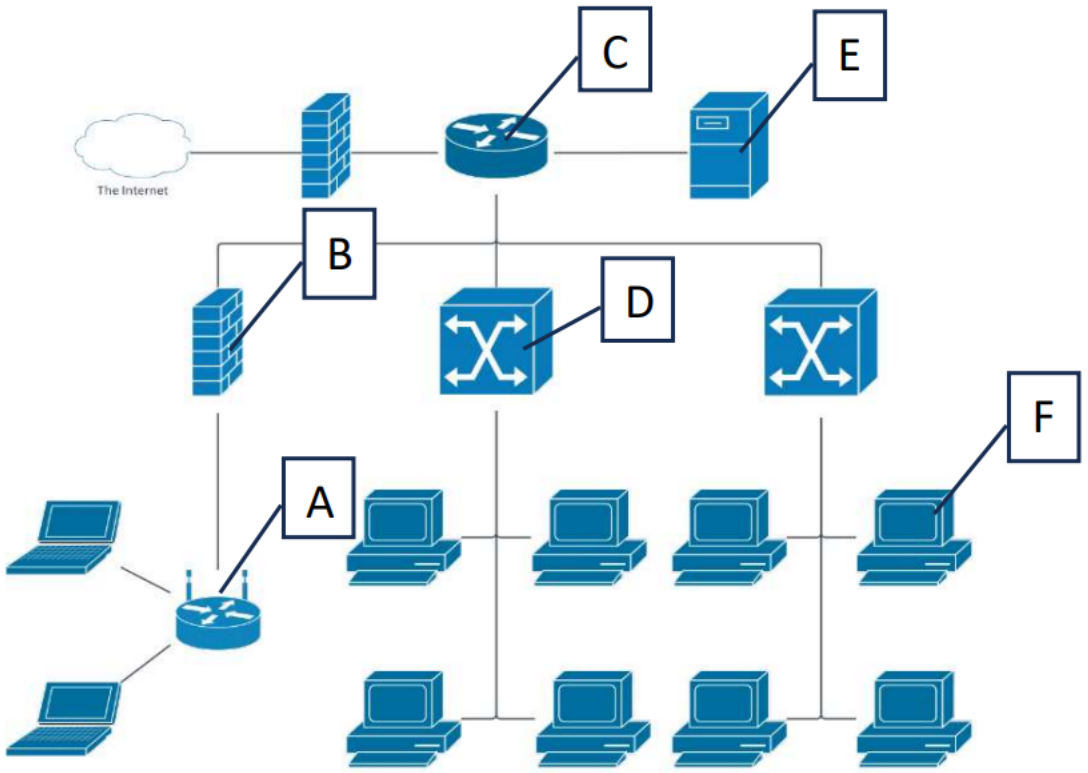
- Ha come indirizzo di rete 160.12.0.0
- Ha come indirizzo di broadcast 160.12.63.255
- Ha come indirizzo di broadcast 160.12.63.254
- Ha come maschera di sottorete 255.255.192.0
- Ha come maschera di sottorete 255.255.186.0
- Lo spazio di indirizzamento arriva sino a (Host Max) 160.12.63.254

(M4.3.2.2) In una Multiutility

- La gestione del cyber rischio è di solito gestito da una commissione o un comitato che risponde al consiglio di amministrazione
- Di solito la responsabilità operativa sulla cybersecurity è in carico ad un CISO che risponde, talvolta indirettamente, ad una direzione di tecnologia o innovazione
- Di solito Presidente, Vicepresidente e Amministratore Delegato hanno uno stesso livello gerarchico
- Di solito solo l'Amministratore delegato risponde al consiglio di amministrazione, mentre il Vicepresidente risponde solo al Presidente
- La proprietà è solo pubblica
- In alcuni casi i sistemi informativi sono esternalizzati in società che rimangono di proprietà dell'azienda

Esercizio 1

Dato il seguente schema topologico:



Inserire negli appositi spazi i nomi dei dispositivi etichettati con le lettere:

A=Router Wi-Fi, B=Firewall, C=Router, D=Switch, E=Server, F=Client

Esercizio 2

L'amministratore di una rete aziendale con indirizzo 210.12.0.0/16 desidera regolare l'accesso bidirezionale da Internet alla rete aziendale consentendo l'accesso dalla rete 150.20.0.0/16 (collaboratori esterni abilitati) alla sottorete interna 210.12.120.0/24 ed impedire alle sottoreti 150.20.20.0/24 e 150.20.40.0/24 (collaboratori non abilitati) di poter accedere alla stessa sottorete interna 210.12.120.0/24, indicare le regole del firewall:

Indice	IP Sorgente	IP Destinatario	Azione
1	150.20.20.0/24	210.12.120.0/24	Blocca
2	150.20.40.0/24	210.12.120.0/24	Blocca
3	150.20.0.0/16	210.12.120.0/24	Consenti
4	0.0.0.0/0	0.0.0.0/0	Blocca